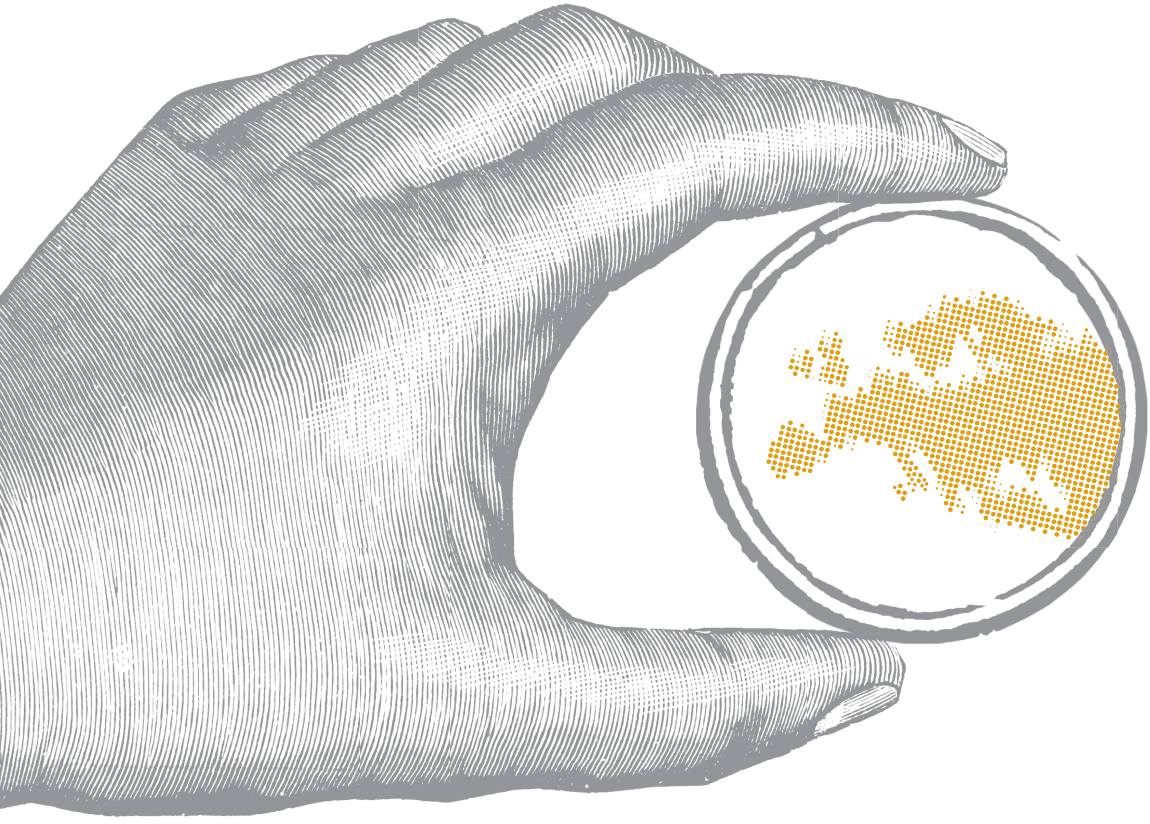
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

CONTRIBUTI

APPLICARE IL GDPR

Le linee guida europee



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza Venezia n. 11 - 00187 Roma
tel: +39-06-696771
fax: +39-06-696773785
e-mail: garante@garanteprivacy.it
posta certificata: protocollo@pec.gpdp.it

www.garanteprivacy.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Applicare il GDPR

Le linee guida europee

www.garanteprivacy.it

Sommario

Prefazione

Il GDPR, ossia il Regolamento generale (Ue) sulla protezione dei dati personali 2016/679, è ormai una realtà con la quale tutti i soggetti pubblici e privati devono confrontarsi nella prassi quotidiana quando vogliono o devono trattare dati personali, per qualsiasi finalità e in qualsiasi contesto. È uno strumento complesso che si inserisce in un solco già aperto dalla direttiva comunitaria del 1995 e, in Italia, dalla legge 675/1996 seguita dal Codice del 2003. Il GDPR conferma e rafforza i principi e i requisiti del precedente quadro normativo, il cui rispetto è condizione essenziale per garantire quello che la nuova architettura dell'Unione ha riconosciuto essere un diritto fondamentale – la protezione dei dati personali. Ma – e questo è uno degli effetti più innovativi - il GDPR responsabilizza titolari e responsabili del trattamento in misura molto superiore al passato, imponendo di pensare in anticipo le finalità e le modalità dei trattamenti e di costruirne correttamente e in modo documentabile l'impalcatura giuridica e organizzativa.

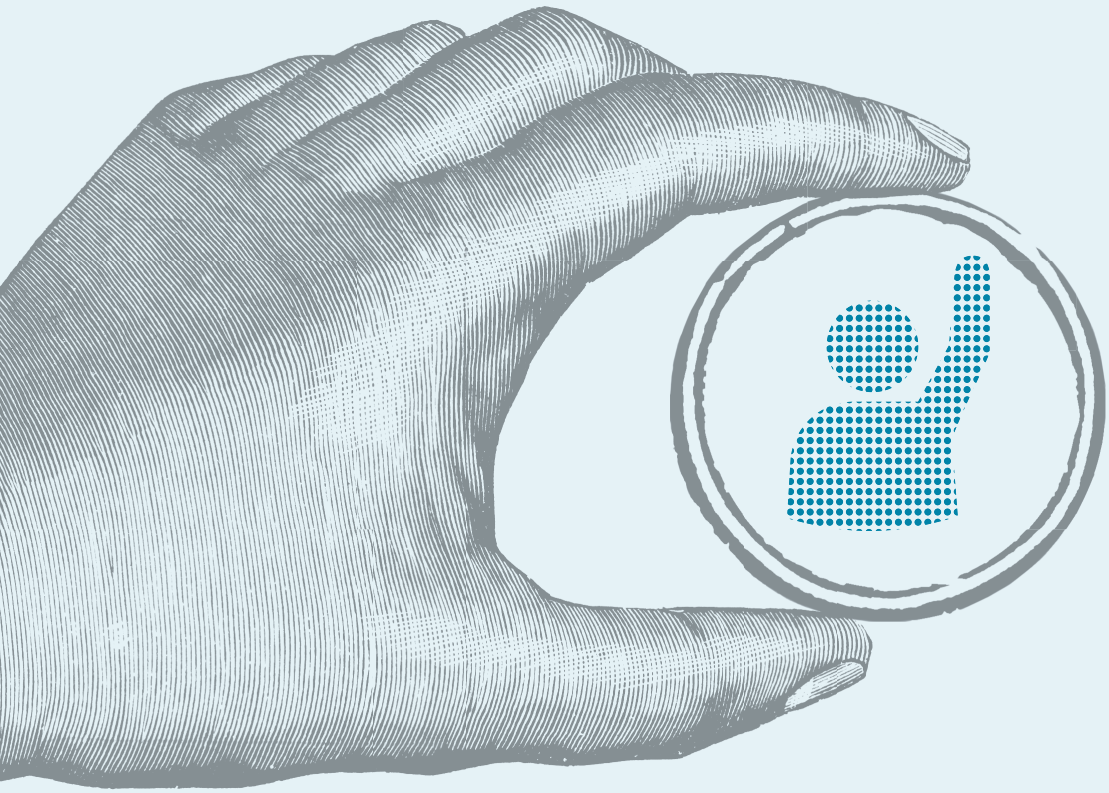
In questa nuova architettura anche le Autorità nazionali di controllo come il Garante trovano conferme e novità: conferme, in quanto Autorità indipendenti e incaricate di garantire la reale attuazione delle norme in tutti gli Stati membri; novità, soprattutto in termini di più stringente ed efficace cooperazione e di obblighi di assistenza reciproca, anche in seno al nuovo organismo creato dal GDPR, il "Comitato europeo per la protezione dei dati" (European Data Protection Board - EDPB). Il Comitato, che ha personalità giuridica e al quale sono demandate funzioni al tempo stesso di guida e di decisore ultimo nei casi controversi, è l'erede del "Gruppo Articolo 29" (WP29), che era stato previsto dalla direttiva del 1995 principalmente come organismo consultivo della Commissione europea e degli stakeholder nazionali. Non per caso il Comitato ha rivisto e fatto proprie - adottandole formalmente - tutte le indicazioni fornite dal WP29 negli ultimi anni in materia di protezione dati e sulla corretta applicazione del GDPR. Ha poi cominciato a sviluppare un nuovo gruppo di linee guida e di altri documenti interpretativi su temi non affrontati sino a quel momento. Come già il Gruppo, il Comitato si compone di un rappresentante per ciascuna Autorità nazionale di controllo (fra cui il Garante), della Commissione europea e del Garante europeo per la protezione dei dati.

In quest'ottica di rinnovamento nella continuità, si è ritenuto utile raccogliere in

una pubblicazione, in versione italiana, tutti i documenti definitivamente approvati dal Comitato e disponibili nel primo anno di vigenza del GDPR, quindi dal 25 maggio 2018. L'obiettivo è quello di fornire uno strumento agile e comprensivo, di consultazione e di riferimento, destinato a tutti coloro che operano nell'ambito della protezione dati: in primo luogo i responsabili della protezione dei dati - RPD (più spesso indicati con l'acronimo inglese DPO), chiamati ad assistere i titolari e responsabili del trattamento nell'individuazione delle prassi corrette per dare attuazione alle norme di protezione dati, e sui quali ricadono quindi obblighi di aggiornamento e conoscenza particolarmente pregnanti. Il volume offre comunque chiarimenti e spunti di riflessione a tutti coloro che vogliano comprendere e tutelare meglio alcuni dei loro diritti fondamentali - come quello alla privacy e alla protezione dati – strumenti di democrazia, prima ancora che facilitatori dell'economia contemporanea.

Si è scelto di non inserire nella raccolta quei documenti per i quali non era disponibile una versione definitiva al 25 maggio 2019, sia perché ancora oggetto di consultazione pubblica, sia perché non ancora perfezionati all'esito di una tale consultazione; tutta la documentazione è comunque rinvenibile sul sito dell'EDPB e su quello del Garante. I documenti sono riprodotti nella loro versione originale, motivo per cui potranno esservi alcune discrepanze soprattutto in termini di stile, ad esempio nell'uso delle maiuscole e minuscole, o di alcuni acronimi. Sono stati raggruppati in quattro macro-aree, rispettivamente concernenti i diritti degli interessati, gli obblighi di titolari e responsabili, i principi relativi ai trasferimenti internazionali di dati personali e, infine, i meccanismi attuativi del GDPR. Completano il volume una sezione contenente link e riferimenti utili, e un mini-glossario dei principali termini e acronimi utilizzati nei testi qui raccolti.

1 I diritti degli interessati



Premessa
I diritti degli interessati

Il GDPR ha, da un lato, rafforzato i diritti riconosciuti agli interessati dalla direttiva 95/46/CE e dal Codice privacy e, dall'altro lato, ha introdotto nuovi diritti come il diritto alla portabilità dei dati.

Le linee-guida sul consenso e quelle sulla trasparenza rappresentano, in questo senso, un esempio significativo. Si tratta di due aspetti del trattamento che sono strettamente connessi perché, pur essendo il consenso uno dei requisiti per trattare lecitamente dati personali e non tanto un diritto degli interessati, il GDPR richiede uno sforzo di trasparenza maggiore da parte dei titolari soprattutto quando vogliano ricorrere al consenso per trattare dati personali. Quindi il WP29 ha chiarito, in particolare, cosa debba intendersi per consenso realmente 'informato', e come si declinano gli obblighi di trasparenza (non solo di informazione) rispetto agli interessati, con particolare riguardo proprio alla prestazione del consenso, anche evidenziando la possibilità di alcune semplificazioni. Peraltro, il GDPR contiene disposizioni molto più stringenti sui contenuti e sulle modalità di redazione delle informative (o meglio, delle "informazioni" destinate agli interessati), e su questo aspetto il documento del WP29 offre numerosi esempi di grande utilità guardando ai diversi contesti. Non si può dimenticare, infine, che molti dubbi hanno accompagnato e accompagnano l'applicazione del requisito di un consenso "esplicito" per il trattamento delle categorie particolari di dati personali di cui agli artt. 9 e 10 del GDPR, e anche su questo punto le linee-guida offrono indicazioni operative ed esempi tratti dalla prassi quotidiana.

Il diritto alla portabilità costituisce indubbiamente (insieme al cosiddetto "diritto all'oblio") una delle maggiori novità del GDPR. E' per questo che il WP29 ha sentito il bisogno di guidare tutti gli stakeholder nella sua corretta applicazione. Sono due, infatti, le componenti essenziali di questo diritto: da un lato, poter ricevere, come interessato, i propri dati personali "forniti" al titolare in qualsiasi modalità e, quindi, anche attraverso la navigazione in rete; dall'altro lato, poter chiedere al titolare del trattamento la trasmissione diretta di tutti

o parte dei propri dati personali a un diverso titolare – purché ciò sia tecnicamente fattibile. Le linee-guida delimitano con maggiore precisione gli ambiti e le interrelazioni di tali componenti e prospettano, fra l'altro, la necessità di un approccio che coinvolga tutti gli stakeholder per consentire la piena estrinsecazione di un diritto che si pone quale strumento importante per la realizzazione di un effettivo controllo diretto sui propri dati personali. Alle linee-guida si accompagnano anche FAQ con l'intento di offrire una rapida panoramica degli aspetti essenziali della portabilità.

Non meno importanti sono le linee-guida del WP29 in materia di profilazione e decisioni automatizzate. Si tratta di temi che, nel corso degli ultimi venti anni, hanno acquistato rilevanza considerevole, sia per la diffusione di servizi basati sulla personalizzazione (attraverso la profilazione di gusti e preferenze degli interessati), sia per l'impiego crescente di tecniche di analisi basate su algoritmi quasi sempre sconosciuti all'interessato e sottratti in larga parte al suo controllo anche quando generano decisioni che influiscono sulla sua sfera personale. Non è un caso, quindi, che il GDPR abbia ritenuto di introdurre una definizione di "profilazione" (non presente nella direttiva del 1995) e di precisare le caratteristiche di un diritto non propriamente nuovo (era infatti già sancito dal Codice privacy italiano e dalla direttiva 95/46/CE), ma certo, come ribadito dal WP29, reso molto più incisivo: quello, per un individuo, di non essere oggetto di una decisione basata esclusivamente su un trattamento automatizzato che comporti effetti importanti (giuridici, ma non solo). In quest'ottica, le linee-guida illustrano anche come debbano interpretarsi i casi in cui questo diritto non si applica, cioè quando si è presenza di determinati presupposti che legittimano decisioni del tipo sopra descritto. Appartengono a questi presupposti il consenso dell'interessato (che deve avere le caratteristiche delineate dal WP29 nelle relative linee-guida) ovvero l'adempimento di obblighi contrattuali assunti dall'interessato (e qui assume eccezionale rilevanza il requisito della "trasparenza") o di obblighi di natura pubblicistica (e qui le linee-guida offrono esempi significativi). Non va dimenticato, infine, che per queste tipologie di trattamento è previsto dallo stesso GDPR il requisito della valutazione di impatto sulla protezione dei dati, che costituisce un'ulteriore garanzia per l'interessato oltre che uno strumento di autotutela per il titolare, cui si offre anche la possibilità di una consultazione preventiva dell'Autorità.

Linee guida sul consenso ai sensi del regolamento (UE) 2016/679 [WP 259 rev. 01]

Adottate il 28 novembre 2017
come modificate e adottate da ultimo il 10 aprile 2018

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 della stessa,

visto il suo regolamento interno,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della Commissione europea, direzione generale Giustizia e consumatori, B - 1049 Bruxelles, Belgio, ufficio MO-59 05/35.

Sito internet: http://ec.europa.eu/justice/data-protection/index_en.htm

Indice

1. INTRODUZIONE

Le presenti linee guida forniscono un'analisi approfondita della nozione di consenso di cui al regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati). Il concetto di consenso di cui alla direttiva sulla protezione dei dati (direttiva 95/46/CE) e alla direttiva relativa alla vita privata e alle comunicazioni elettroniche (direttiva 2002/58/CE) si è evoluto. Il regolamento generale sulla protezione dei dati fornisce ulteriori chiarimenti e specifiche sui requisiti per ottenere e dimostrare un consenso valido. Prendendo le mosse dal parere 15/2011 sul consenso, le presenti linee guida si concentrano sui cambiamenti introdotti, fornendo orientamenti pratici per garantire il rispetto del regolamento. Il titolare del trattamento è tenuto a innovare per trovare soluzioni che siano conformi ai requisiti di legge e sostengano meglio la protezione dei dati personali e gli interessi degli interessati.

Il consenso rimane una delle sei basi legittime per trattare i dati personali, come disposto dall'articolo 6 del regolamento[1]. Prima di avviare attività che implicano il trattamento di dati personali, il titolare del trattamento deve sempre valutare con attenzione la base legittima appropriata per il trattamento.

Di norma, il consenso può costituire la base legittima appropriata solo se all'interessato vengono offerti il controllo e l'effettiva possibilità di scegliere se accettare o meno i termini proposti o rifiutarli senza subire pregiudizio. Quando richiede il consenso, il titolare del trattamento deve valutare se soddisferà tutti i requisiti per essere valido. Se ottenuto nel pieno rispetto del regolamento, il consenso è uno strumento che fornisce all'interessato il controllo sul trattamento dei dati personali che lo riguardano. In caso contrario, il controllo diventa illusorio e il consenso non costituirà una base valida per il trattamento, rendendo illecita l'attività di trattamento[2].

Ove coerenti con il nuovo quadro giuridico, i pareri che il Gruppo di lavoro Articolo 29 (in appresso: Gruppo di lavoro) ha formulato in materia di consenso[3] rimangono pertinenti, in quanto il regolamento generale sulla protezione dei dati codifica gli orientamenti e le buone prassi generali del Gruppo di lavoro e lascia immutata la maggior parte degli aspetti essenziali del consenso. Di conseguenza, il presente documento amplia e completa pareri precedenti del Gruppo di lavoro su argomenti specifici che fanno riferimento al consenso ai sensi della direttiva 95/46/CE, senza sostituirli.

Come affermato nel parere 15/2011 sulla definizione di consenso, l'invito ad accettare il trattamento dei dati dovrebbe essere soggetto a criteri rigorosi, poiché sono in gioco i diritti fondamentali dell'interessato e il titolare del trattamento intende svolgere un trattamento che senza il consenso sarebbe illecito[4]. Il ruolo cruciale del consenso è sottolineato dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. Inoltre, l'ottenimento del consenso non fa venir meno né diminuisce in alcun modo l'obbligo del titolare del trattamento di rispettare i principi applicabili al trattamento sanciti nel regolamento generale sulla protezione dei dati, in particolare all'articolo 5,

per quanto concerne la correttezza, la necessità e la proporzionalità, nonché la qualità dei dati. Il fatto che il trattamento dei dati personali si basi sul consenso dell'interessato non legittima la raccolta di dati non necessari a una finalità specifica di trattamento, che sarebbe fondamentalmente iniqua[5].

Parallelamente, il Gruppo di lavoro è a conoscenza della revisione della direttiva relativa alla vita privata e alle comunicazioni elettroniche. La nozione di consenso nel progetto di regolamento sulla vita privata e le comunicazioni elettroniche rimane legata a quella del regolamento generale sulla protezione dei dati[6]. È probabile che ai sensi del futuro strumento le organizzazioni necessitino del consenso per la maggior parte dei messaggi di marketing online, per le chiamate di marketing e per i metodi di tracciamento online, compreso tramite l'uso di cookie, applicazioni o altri software. Il Gruppo di lavoro ha già fornito raccomandazioni e orientamenti al legislatore europeo in merito alla proposta di regolamento sulla vita privata e le comunicazioni elettroniche[7].

Per quanto riguarda l'attuale direttiva relativa alla vita privata e alle comunicazioni elettroniche, il Gruppo di lavoro rileva che i riferimenti alla direttiva 95/46/CE abrogata si intendono fatti al regolamento generale sulla protezione dei dati[8]. Ciò vale anche per i riferimenti riguardanti il consenso, poiché il regolamento sulla vita privata e le comunicazioni elettroniche non sarà (ancora) entrato in vigore il 25 maggio 2018. Ai sensi dell'articolo 95 del regolamento generale sulla protezione dei dati, non sono imposti obblighi supplementari in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione, nella misura in cui la direttiva relativa alla vita privata e alle comunicazioni elettroniche impone obblighi specifici aventi il medesimo obiettivo. Il Gruppo di lavoro rileva che i requisiti per il consenso ai sensi del regolamento generale sulla protezione dei dati non sono considerati un "obbligo supplementare", bensì condizioni preliminari per la liceità del trattamento. Pertanto, tali requisiti sono applicabili alle situazioni che rientrano nel campo di applicazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

2. CONSENSO DI CUI ALL'ARTICOLO 4, PUNTO 11, DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

L'articolo 4, punto 11, del regolamento generale sulla protezione dei dati definisce il consenso dell'interessato come: *"qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento"*.

La nozione di consenso rimane sostanzialmente simile a quella della direttiva 95/46/CE, e il consenso rimane uno dei presupposti per il trattamento dei dati personali, ai sensi dell'articolo 6 del regolamento generale sulla protezione dei dati[9]. Oltre alla definizione modificata di cui all'articolo 4, punto 11, il regola-

mento fornisce ulteriori indicazioni, all'articolo 7 e ai considerando 32, 33, 42 e 43, su come il titolare del trattamento deve agire per rispettare gli elementi principali del requisito del consenso.

L'inclusione, nel regolamento, di disposizioni e considerando specifici sulla revoca del consenso conferma che quest'ultimo dovrebbe essere una decisione reversibile e che l'interessato mantiene un certo grado di controllo.

3. ELEMENTI DEL CONSENSO VALIDO

L'articolo 4, punto 11, del regolamento generale sulla protezione dei dati stabilisce che il consenso dell'interessato è qualsiasi:

- manifestazione di volontà libera,
- specifica,
- informata e
- inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Le sezioni che seguono analizzano la misura in cui la formulazione dell'articolo 4, punto 11, richiede al titolare del trattamento di modificare le sue richieste/i suoi moduli di consenso affinché siano conformi al regolamento generale sulla protezione dei dati[10].

3.1. CONSENSO LIBERO/MANIFESTAZIONE DI VOLONTÀ LIBERA[11]

L'elemento della manifestazione di volontà "libera" implica che l'interessato abbia una scelta effettiva e il controllo sui propri dati. Come regola generale, il regolamento stabilisce che se l'interessato non dispone di una scelta effettiva, si sente obbligato ad acconsentire o subirà conseguenze negative se non acconsente, il consenso non sarà valido[12]. Se il consenso è parte non negoziabile delle condizioni generali di contratto/servizio, si presume che non sia stato prestato liberamente. Di conseguenza, il consenso non sarà considerato libero se l'interessato non può rifiutarlo o revocarlo senza subire pregiudizio[13]. Il regolamento generale sulla protezione dei dati ha preso in considerazione anche la nozione di squilibrio tra il titolare del trattamento e l'interessato.

Nel valutare se il consenso sia stato prestato liberamente, si deve anche tener conto dell'eventualità che il consenso sia collegato all'esecuzione di un contratto o alla prestazione di un servizio come descritto all'articolo 7, paragrafo 4. L'articolo 7, paragrafo 4, contenendo l'inciso "tra le altre", non esaustivo e può quindi comprendere altre eventualità. In termini generali, qualsiasi azione di pressione o influenza inappropriata sull'interessato (che si può manifestare in svariati modi) che impedisca a quest'ultimo di esercitare il suo libero arbitrio, rende il consenso invalido.

[Esempio 1]
Un'applicazione mobile per il fotoritocco chiede agli utenti di attivare la localizzazione GPS per l'utilizzo dei suoi servizi. L'applicazione comunica agli utenti che utilizzerà i dati raccolti per finalità di pubblicità comportamentale. Né la geolocalizzazione né la pubblicità comportamentale online sono necessarie per la prestazione del servizio di fotoritocco e vanno oltre la fornitura del servizio principale. Poiché gli utenti non possono utilizzare l'applicazione senza acconsentire a tali finalità, il consenso non può essere considerato liberamente espresso.

3.1.1. SQUILIBRIO DI POTERE

Il considerando 43[14] indica chiaramente che è improbabile che le **autorità pubbliche** possano basarsi sul consenso per effettuare il trattamento, poiché quando il titolare del trattamento è un'autorità pubblica sussiste spesso un evidente squilibrio di potere nella relazione tra il titolare del trattamento e l'interessato. In molti di questi casi è inoltre evidente che l'interessato non dispone di alternative realistiche all'accettazione (dei termini) del trattamento. Il Gruppo di lavoro ritiene che esistano altre basi legittime, in linea di principio più appropriate, per il trattamento da parte delle autorità pubbliche[15].

Fatte salve queste considerazioni generali, il regolamento non esclude completamente il ricorso al consenso come base legittima per il trattamento dei dati da parte delle autorità pubbliche. I seguenti esempi mostrano infatti che l'uso del consenso può essere appropriato in determinate circostanze.

[Esempio 2]
Un comune sta pianificando l'esecuzione di lavori di manutenzione stradale. Poiché i lavori possono perturbare il traffico per parecchio tempo, il comune offre ai cittadini la possibilità di iscriversi a una mailing list per ricevere aggiornamenti sull'avanzamento dei lavori e sui ritardi previsti. Il comune chiarisce che la partecipazione non è obbligatoria e chiede il consenso a utilizzare gli indirizzi di posta elettronica per questa finalità (esclusiva). I cittadini che non acconsentono non perderanno l'accesso ad alcun servizio fondamentale del comune né alcun diritto, di conseguenza possono esprimere o rifiutare liberamente il loro consenso a questo uso dei dati. Tutte le informazioni sui lavori stradali saranno disponibili anche sul sito web del comune.

[Esempio 3]
Un proprietario terriero necessita di alcuni permessi tanto dal comune quanto dalla provincia. Entrambi gli enti pubblici richiedono le stesse informazioni per il rilascio dei permessi, ma non hanno accesso alle rispettive banche dati. Di conseguenza entrambi chiedono le stesse informazioni e il proprietario terriero invia i dati ad entrambi. Il comune e la provincia chiedono il consenso dell'interessato per riunire i fascicoli al fine di evitare duplicazioni di procedure e corrispondenza. Entrambi gli enti pubblici assicurano che ciò è facoltativo e che le richieste di permesso verranno comunque trattate separatamente qualora l'interessato de-

cida di non acconsentire alla riunione dei fascicoli. Il proprietario terriero può quindi esprimere liberamente il consenso alle autorità per la finalità di riunione dei fascicoli.

[Esempio 4]
Una scuola pubblica chiede agli studenti il consenso ad utilizzare le loro fotografie in una rivista studentesca in formato cartaceo. In questo caso il consenso costituisce una scelta vera e propria a condizione che agli studenti non vengano negati l'istruzione o altri servizi e che gli studenti possano rifiutare il consenso senza subire pregiudizio[16].

Lo squilibrio di potere sussiste anche nel contesto dell'**occupazione**[17]. Data la dipendenza risultante dal rapporto datore di lavoro/dipendente, è improbabile che l'interessato sia in grado di negare al datore di lavoro il consenso al trattamento dei dati senza temere o rischiare di subire ripercussioni negative come conseguenza del rifiuto. È improbabile che il dipendente sia in grado di rispondere liberamente, senza percepire pressioni, alla richiesta del datore di lavoro di acconsentire, ad esempio, all'attivazione di sistemi di monitoraggio, quali la sorveglianza con telecamere sul posto di lavoro, o alla compilazione di moduli di valutazione[18]. Di conseguenza il Gruppo di lavoro ritiene problematico per il datore di lavoro trattare i dati personali dei dipendenti attuali o futuri sulla base del consenso, in quanto è improbabile che questo venga prestato liberamente. Per la maggior parte delle attività di trattamento svolte sul posto di lavoro, la base legittima non può e non dovrebbe essere il consenso del dipendente (articolo 6, paragrafo 1, lettera a)) in considerazione della natura del rapporto tra datore di lavoro e dipendente[19].

Tuttavia, ciò non significa che il datore di lavoro non possa mai basarsi sul consenso come base legittima per il trattamento. In alcune situazioni il datore di lavoro è in grado di dimostrare che il consenso è stato effettivamente espresso liberamente. Dato lo squilibrio di potere tra il datore di lavoro e il suo personale, i dipendenti possono manifestare il loro consenso liberamente soltanto in casi eccezionali, quando non subiranno alcuna ripercussione negativa per il fatto che esprimano il loro consenso o meno[20].

[Esempio 5]
Una troupe cinematografica filmerà una determinata area di un ufficio. Il datore di lavoro chiede a tutti i dipendenti che hanno la scrivania in quella zona il consenso a essere ripresi, in quanto potrebbero apparire sullo sfondo del video. Chi non vuole essere filmato non viene penalizzato in alcun modo e ottiene invece una scrivania altrove nell'edificio per l'intera durata delle riprese.

Gli squilibri di potere non sono limitati alle autorità pubbliche e ai datori di lavoro, potendo verificarsi anche in altre situazioni. Come evidenziato dal Gruppo di lavoro in diversi pareri, il consenso è valido soltanto se l'interessato è in grado di operare realmente una scelta e non c'è il rischio di raggiri, intimidazioni, coercizioni o conseguenze negative significative (ad es. costi aggiuntivi sostanziali) in caso di rifiuto a prestare il consenso. Il consenso non sarà con-

siderato liberamente espresso qualora vi sia qualsiasi elemento di costrizione, pressione o incapacità di esercitare il libero arbitrio.

3.1.2. CONDIZIONALITÀ

Per valutare se il consenso sia stato prestato liberamente è di rilievo l'articolo 7, paragrafo 4, del regolamento[21].
L'articolo 7, paragrafo 4, indica, tra l'altro, che è altamente inopportuno "accorpare" il consenso all'accettazione delle condizioni generali di contratto/servizio o "subordinare" la fornitura di un contratto o servizio a una richiesta di consenso al trattamento di dati personali che non sono necessari per l'esecuzione del contratto o servizio. Si presume che il consenso prestato in una tale situazione non sia stato espresso liberamente (considerando 43). L'articolo 7, paragrafo 4, mira a garantire che la finalità del trattamento dei dati personali non sia mascherata né accorpata all'esecuzione di un contratto o alla prestazione di un servizio per il quale i dati personali non sono necessari. In tal modo, il regolamento assicura che il trattamento dei dati personali per cui viene richiesto il consenso non possa trasformarsi direttamente o indirettamente in una controprestazione contrattuale. Le due basi legittime per la liceità del trattamento dei dati personali, ossia il consenso e l'esecuzione di un contratto, non possono essere riunite e rese indistinte.

L'obbligo di acconsentire all'uso di dati personali aggiuntivi rispetto a quelli strettamente necessari limita la scelta dell'interessato e ostacola l'espressione del libero consenso. Poiché la legislazione in materia di protezione dei dati mira a tutelare i diritti fondamentali, è essenziale che l'interessato abbia il controllo sui propri dati personali; inoltre sussiste una presunzione forte secondo cui il consenso a un trattamento di dati personali non necessario non può essere considerato un corrispettivo obbligatorio dell'esecuzione di un contratto o della prestazione di un servizio.

Pertanto, ogni volta che una richiesta di consenso è legata all'esecuzione di un contratto da parte del titolare del trattamento, l'interessato che non desidera mettere a disposizione i propri dati personali per il trattamento da parte del titolare corre il rischio di vedersi negare l'erogazione dei servizi richiesti.

Per valutare se si verifica una situazione di accorpamento o subordinazione è importante determinare qual è la portata del contratto e quali dati sono necessari per la sua esecuzione. Secondo il parere 06/2014 del Gruppo di lavoro, l'espressione "necessario per l'esecuzione di un contratto" deve essere interpretata in maniera rigorosa. Il trattamento deve essere necessario per adempiere il contratto con ciascun interessato. In quest'ambito possono rientrare, per esempio, il trattamento dell'indirizzo dell'interessato ai fini della consegna delle merci acquistate online o il trattamento degli estremi della carta di credito per facilitare il pagamento. Nel contesto occupazionale, questo presupposto potrebbe permettere, per esempio, il trattamento di informazioni riguardanti lo stipendio e le coordinate bancarie per consentire il pagamento degli stipen-

di[22]. È necessario che vi sia un collegamento diretto e obiettivo tra il trattamento dei dati e la finalità dell'esecuzione del contratto.

Quando il titolare del trattamento intende trattare dati personali che sono effettivamente necessari per l'esecuzione di un contratto il consenso non è la base legittima appropriata[23].

L'articolo 7, paragrafo 4, è pertinente soltanto laddove i dati richiesti **non** sono necessari per l'esecuzione del contratto (ivi compreso per la prestazione di un servizio) e l'esecuzione del contratto è subordinata all'ottenimento di tali dati in base al presupposto del consenso. Al contrario, qualora il trattamento sia necessario per eseguire il contratto (ivi incluso per la prestazione di un servizio), l'articolo 7, paragrafo 4, non si applica.

> ***[Esempio 6]***
> *Una banca chiede ai clienti il consenso per consentire a terzi di utilizzare i dettagli di pagamento per finalità di marketing diretto. Questa attività di trattamento non è necessaria per l'esecuzione del contratto stipulato con il cliente e la prestazione di servizi ordinari di conto bancario. Qualora il rifiuto del cliente a prestare il consenso per tale finalità di trattamento porti alla negazione di servizi bancari, alla chiusura del conto bancario o, a seconda dei casi, a un aumento della commissione, il consenso non può considerarsi espresso liberamente.*

La scelta del legislatore di evidenziare la condizionalità, tra l'altro, come presunzione di mancanza di libertà di esprimere il consenso dimostra che il verificarsi della condizionalità deve essere attentamente esaminato. L'espressione "nella massima considerazione" di cui all'articolo 7, paragrafo 4, suggerisce che il titolare del trattamento deve prestare particolare attenzione qualora il contratto (che potrebbe includere la prestazione di un servizio) sia collegato a una richiesta di consenso al trattamento di dati personali.

Poiché l'articolo 7, paragrafo 4, non è formulato in maniera assoluta, in un numero molto ristretto di casi tale condizionalità potrebbe non rendere invalido il consenso. Tuttavia, il verbo "si presume" al considerando 43 indica chiaramente che tali casi saranno estremamente eccezionali.

Ad ogni modo, l'onere della prova riguardo all'articolo 7, paragrafo 4, incombe al titolare del trattamento[24]. Questa norma specifica riflette il principio generale di responsabilizzazione che permea l'intero regolamento generale sulla protezione dei dati. Tuttavia, quando si applica l'articolo 7, paragrafo 4, risulta più difficile per il titolare del trattamento dimostrare che l'interessato ha prestato liberamente il consenso[25].

Il titolare del trattamento potrebbe sostenere che la sua organizzazione offre all'interessato una scelta reale mettendolo in grado di scegliere tra un servizio che prevede il consenso all'uso dei dati personali per finalità supplementari, da un lato, e un servizio equivalente che non implica un siffatto consenso, dall'altro. Finché esiste la possibilità che il contratto venga eseguito o che il

servizio oggetto del contratto venga prestato dal titolare del trattamento senza necessità di acconsentire ad usi ulteriori o supplementari dei dati in questione non si è in presenza di un servizio condizionato. Tuttavia, i due servizi devono essere effettivamente equivalenti.

Il Gruppo di lavoro ritiene che il consenso non possa considerarsi prestato liberamente se il titolare del trattamento sostiene che esiste una scelta tra il suo servizio che prevede il consenso all'uso dei dati personali per finalità supplementari, da un lato, e un servizio equivalente offerto da un altro titolare del trattamento, dall'altro. In tal caso la libertà di scelta dipenderebbe dagli altri operatori del mercato e dal fatto che l'interessato ritenga che i servizi offerti dall'altro titolare del trattamento siano effettivamente equivalenti. Ciò implicherebbe inoltre l'obbligo per il titolare del trattamento di monitorare gli sviluppi del mercato per garantire la continuità della validità del consenso per le sue attività di trattamento dei dati, in quanto un concorrente potrebbe modificare il suo servizio in un momento successivo. Di conseguenza il consenso ottenuto con questa argomentazione non rispetta il regolamento generale sulla protezione dei dati.

3.1.3. GRANULARITÀ

Un servizio può comportare trattamenti multipli per più finalità. In tal caso, l'interessato dovrebbe essere libero di scegliere quale finalità accettare anziché dover acconsentire a un insieme di finalità. Ai sensi del regolamento generale sulla protezione dei dati, in un determinato caso possono essere giustificati più consensi per iniziare a offrire un servizio.

Il considerando 43 chiarisce che si presume che il consenso non sia stato espresso liberamente se il processo o la procedura seguiti per ottenerlo non permettono all'interessato di esprimere un consenso separato ai distinti trattamenti dei dati personali (ad esempio solo ad alcuni trattamenti e non ad altri) nonostante ciò sia appropriato nel singolo caso. Il considerando 32 afferma: *"Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste"*.

Se il titolare del trattamento ha riunito diverse finalità di trattamento e non ha chiesto il consenso separato per ciascuna di esse non c'è libertà. La granularità è strettamente correlata alla necessità che il consenso sia specifico, come analizzato nella sezione 3.2. Quando il trattamento di dati mira a perseguire finalità diverse, la soluzione per soddisfare le condizioni per la validità del consenso risiede nella granularità, ossia nella separazione delle finalità e nell'ottenimento del consenso per ciascuna di esse.

[Esempio 7]
Nel contesto della medesima richiesta di consenso, un rivenditore chiede ai propri clienti il consenso a utilizzare i loro dati per inviare comunicazioni di marke-

ting tramite posta elettronica e per condividere i dati con altre società del gruppo. Tale consenso non è granulare in quanto non è distinto per queste due finalità, pertanto non sarà valido. In questo caso è necessario un consenso specifico all'invio dei dati di contatto ai partner commerciali. Tale consenso specifico sarà ritenuto valido per ciascun partner (cfr. anche la sezione 3.3.1) la cui identità è stata fornita all'interessato al momento dell'ottenimento del consenso, nella misura in cui i dati vengano inviati per la medesima finalità (nell'esempio, finalità di marketing).

3.1.4. PREGIUDIZIO

Il titolare del trattamento deve dimostrare che è possibile rifiutare il consenso oppure revocarlo senza subire pregiudizio (considerando 42), ad esempio dimostrando che la revoca del consenso non comporta alcun costo per l'interessato e quindi nessuno svantaggio evidente in caso di revoca.

Altri esempi di pregiudizio sono l'inganno, l'intimidazione, la coercizione o conseguenze negative significative in caso di mancato consenso. Il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha potuto scegliere liberamente o realmente se acconsentire o meno e che poteva revocare il consenso senza pregiudizio.

Se il titolare del trattamento può dimostrare che il servizio consente di revocare il consenso senza conseguenze negative, ad esempio senza che il livello della prestazione del servizio venga diminuito a scapito dell'utente, allora può dimostrare che il consenso è stato conferito liberamente. Il regolamento generale sulla protezione dei dati non esclude tutti gli incentivi, tuttavia spetta al titolare del trattamento dimostrare che il consenso è stato prestato liberamente in tutte le circostanze.

[Esempio 8]
Un'applicazione mobile dedicata allo stile di vita richiede, all'atto dello scaricamento, il consenso all'accesso all'accelerometro del telefono. Tale accesso non è necessario per il funzionamento dell'applicazione, ma è utile al titolare del trattamento per saperne di più sui movimenti e sui livelli di attività degli utenti. Un utente revoca il consenso e scopre che dopo la revoca l'applicazione funziona solo in misura limitata. Questo è un esempio di pregiudizio ai sensi del considerando 42, il che significa che il consenso non è mai stato ottenuto in maniera valida (e quindi il titolare del trattamento deve cancellare tutti i dati personali sui movimenti degli utenti raccolti in tale modo).

[Esempio 9]
Un interessato si iscrive alla newsletter di un rivenditore del settore della moda che offre sconti generali. Il rivenditore chiede all'interessato il consenso per raccogliere ulteriori dati sulle preferenze di acquisto in maniera da personalizzare le offerte in base alle preferenze dell'interessato secondo la cronologia degli acquisti o un questionario facoltativo. Quando l'interessato successivamente revoca il

consenso, riceve nuovamente sconti per articoli di moda non personalizzati. Ciò non equivale a un pregiudizio in quanto l'interessato ha perso soltanto l'incentivo ammissibile.

[Esempio 10]
Una rivista di moda offre ai lettori la possibilità di acquistare nuovi prodotti per il trucco prima del loro lancio ufficiale.
I prodotti saranno presto disponibili per la vendita, ma i lettori della rivista ne riceveranno un'anteprima esclusiva. Per godere di tale vantaggio i lettori devono fornire l'indirizzo postale e accettare l'iscrizione alla mailing list della rivista. L'indirizzo postale è necessario per la spedizione e la mailing list viene utilizzata per l'invio di offerte commerciali per prodotti quali cosmetici o t-shirt nel corso dell'anno.
L'azienda spiega che i dati relativi alla mailing list saranno utilizzati esclusivamente per l'invio di prodotti e pubblicità cartacea da parte della rivista stessa e non saranno condivisi con altre organizzazioni.
Qualora non voglia comunicare il proprio indirizzo per tale finalità, il lettore non subisce alcun pregiudizio in quanto i prodotti saranno comunque a sua disposizione.

3.2. SPECIFICO

L'articolo 6, paragrafo 1, lettera a), conferma che il consenso dell'interessato deve essere espresso in relazione a "una o più specifiche" finalità e che l'interessato deve poter scegliere in relazione a ciascuna di esse[26]. Il requisito secondo il quale il consenso deve essere "specifico" mira a garantire un certo grado di controllo da parte dell'utente e trasparenza per l'interessato. Tale requisito non è stato modificato dal regolamento e rimane strettamente legato al requisito del consenso "informato". Allo stesso tempo, deve essere interpretato in linea con il requisito della "granularità", affinché il consenso sia "libero"[27]. In sintesi, per rispettare l'elemento della specificità ("specifico"), il titolare del trattamento deve applicare:

I) la specificazione delle finalità come garanzia contro la "*function creep*", ossia l'estensione indebita delle funzionalità;
II) la granularità nelle richieste di consenso, e
III) una chiara separazione delle informazioni sull'ottenimento del consenso per le attività di trattamento dei dati rispetto alle informazioni su altre questioni.

Sul punto I): ai sensi dell'articolo 5, paragrafo 1, lettera b), del regolamento, per ottenere un consenso valido occorre sempre prima determinare la finalità specifica, esplicita e legittima dell'attività di trattamento prevista[28]. La necessità di un consenso specifico associata alla nozione di limitazione delle finalità di cui all'articolo 5, paragrafo 1, lettera b), funge da garanzia contro l'ampliamento progressivo, o la commistione, delle finalità di trattamento dei dati dopo che l'interessato ha acconsentito alla loro raccolta iniziale. Questo fenomeno, noto anche come "*function creep*", rappresenta un rischio per l'interessato, in

quanto può comportare l'uso non previsto di dati personali da parte del titolare del trattamento o di terzi e la perdita del controllo da parte dell'interessato.

Se il titolare del trattamento si basa sull'articolo 6, paragrafo 1, lettera a), l'interessato deve sempre fornire il consenso per una finalità di trattamento specifica[29]. In linea con il concetto di *limitazione delle finalità* e con l'articolo 5, paragrafo 1, lettera b), e il considerando 32 del regolamento, il consenso può coprire trattamenti distinti, purché abbiano la medesima finalità. Chiaramente il consenso specifico può essere ottenuto soltanto quando l'interessato è specificamente informato delle finalità previste dell'uso dei dati che lo riguardano.

Nonostante le disposizioni in materia di compatibilità delle finalità, il consenso deve essere specifico per finalità. L'interessato presterà il consenso nella convinzione di avere il controllo sui suoi dati e nella convinzione che questi saranno trattati esclusivamente per le finalità specificate. Se tratta i dati basandosi sul presupposto del consenso e intende trattarli per un'altra finalità, il titolare del trattamento deve richiedere un ulteriore consenso per tale finalità a meno che non possa basarsi su un'altra base legittima che risponda meglio alla situazione.

> ***[Esempio 11]***
> *Una rete TV via cavo raccoglie i dati personali degli abbonati, sulla base del loro consenso, per fornire suggerimenti personali su nuovi film che, stando alle abitudini di visualizzazione, potrebbero interessare loro. Dopo un po', la rete TV vorrebbe consentire a terzi di inviare (o mostrare) pubblicità mirata sulla base delle abitudini di visualizzazione degli abbonati. Data questa nuova finalità, è necessario ottenere un nuovo consenso.*

Sul punto II): i meccanismi di consenso devono essere granulari non solo per soddisfare il requisito del consenso "libero", ma anche per soddisfare quello del consenso "specifico". Ciò significa che il titolare del trattamento che richiede il consenso per finalità diverse dovrebbe prevedere una possibilità di adesione distinta per ciascuna finalità, in modo da consentire all'utente di esprimere un consenso specifico per le finalità specifiche.

Sul punto III): il titolare del trattamento dovrebbe fornire informazioni specifiche, in relazione a ciascuna richiesta di consenso distinta, sui dati che vengono trattati per ciascuna finalità, al fine di rendere noto all'interessato l'impatto delle diverse scelte a sua disposizione. In questo modo l'interessato può esprimere un consenso specifico. Questo aspetto si sovrappone al requisito che impone al titolare del trattamento di fornire informazioni chiare, come analizzato al punto 3.3.

3.3. INFORMATO

Il regolamento generale sulla protezione dei dati rafforza il requisito secondo cui il consenso deve essere informato. Ai sensi dell'articolo 5 del regolamen-

to, il requisito della trasparenza è uno dei principi fondamentali, strettamente legato ai principi di correttezza e liceità. Fornire informazioni agli interessati prima di ottenerne il consenso è fondamentale per consentire loro di prendere decisioni informate, capire a cosa stanno acconsentendo e, ad esempio, esercitare il diritto di revocare il consenso. Se il titolare del trattamento non fornisce informazioni accessibili, il controllo dell'utente diventa illusorio e il consenso non costituirà una base valida per il trattamento.

Se i requisiti per il consenso informato non sono rispettati il consenso non sarà valido e il titolare del trattamento potrebbe essere in violazione dell'articolo 6 del regolamento.

3.3.1. REQUISITI MINIMI DI CONTENUTO DEL CONSENSO "INFORMATO"

Affinché il consenso sia informato è necessario informare l'interessato su determinati elementi che sono fondamentali per effettuare una scelta. Di conseguenza, il Gruppo di lavoro ritiene che per ottenere un consenso valido siano necessarie almeno le seguenti informazioni:

I) l'identità del titolare del trattamento[30];
II) la finalità di ciascuno dei trattamenti per i quali è richiesto il consenso[31];
III) quali (tipi di) dati saranno raccolti e utilizzati[32];
IV) l'esistenza del diritto di revocare il consenso[33];
V) informazioni sull'uso dei dati per un processo decisionale automatizzato ai sensi dell'articolo 22, paragrafo 2, lettera c)[34], se del caso; e
VI) informazioni sui possibili rischi di trasferimenti di dati dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate come descritto nell'articolo 46[35].

Per quanto riguarda i punti i) e iii), il Gruppo di lavoro osserva che qualora più titolari del trattamento (congiunti) intendano basarsi sul medesimo consenso oppure qualora i dati debbano essere trasferiti o trattati da altri titolari del trattamento che intendono basarsi sul consenso iniziale, tutti questi titolari del trattamento devono essere indicati. Non è necessario fornire i nomi dei responsabili del trattamento, sebbene per rispettare gli articoli 13 e 14 del regolamento il titolare del trattamento dovrà fornire un elenco completo dei destinatari o delle categorie di destinatari, inclusi i responsabili del trattamento. Per concludere, il Gruppo di lavoro rileva che, a seconda delle circostanze e del contesto della fattispecie, potrebbero essere necessarie più informazioni per consentire all'interessato di comprendere veramente i trattamenti in corso.

3.3.2. COME FORNIRE LE INFORMAZIONI

Il regolamento generale sulla protezione dei dati non prescrive la forma o il formato in cui è necessario fornire le informazioni affinché sia soddisfatto il requisito del consenso informato. Le informazioni valide possono quindi essere presentate in vari modi, ad esempio sotto forma di dichiarazioni scritte

o verbali oppure di messaggi audio o video. Tuttavia, il regolamento prevede varie prescrizioni in merito al consenso informato, in particolare all'articolo 7, paragrafo 2, e al considerando 32. Ciò assicura un maggiore livello di chiarezza e accessibilità delle informazioni.

Quando richiede il consenso, il titolare del trattamento dovrebbe assicurarsi di usare sempre un linguaggio chiaro e semplice. Ciò significa che il messaggio dovrebbe essere facilmente comprensibile per una persona media, non solo per un avvocato. Il titolare del trattamento non può usare lunghe politiche sulla tutela della vita privata difficili da comprendere oppure informative piene di gergo giuridico. Il consenso deve essere chiaro e distinguibile dalle altre questioni, e deve essere presentato in una forma intelligibile e facilmente accessibile. Ciò significa, in sostanza, che le informazioni pertinenti per prendere una decisione informata sul consenso non possono essere nascoste all'interno delle condizioni generali di contratto/servizio[36].

Il titolare del trattamento deve garantire che il consenso sia fornito sulla base di informazioni che consentono all'interessato di identificare facilmente chi è il titolare del trattamento e di capire a cosa sta acconsentendo. Il titolare del trattamento deve descrivere chiaramente la finalità del trattamento dei dati per la quale richiede il consenso[37].

Ulteriori orientamenti specifici in materia di accessibilità sono stati forniti dal Gruppo di lavoro nelle linee guida sulla trasparenza. Quando il consenso deve essere prestato per via elettronica, la richiesta deve essere chiara e concisa. La messa a disposizione di informazioni "a livelli" e granulari può essere un modo appropriato per soddisfare il duplice obbligo di essere precisi e completi, da un lato, e comprensibili, dall'altro.

Il titolare del trattamento deve valutare il tipo di pubblico che fornisce dati personali alla sua organizzazione. Ad esempio, se il pubblico di destinazione include interessati minorenni, il titolare del trattamento deve assicurarsi che le informazioni siano comprensibili per i minori[38]. Dopo aver individuato il pubblico, il titolare del trattamento deve stabilire le informazioni da fornire e, successivamente, il modo in cui fornirle.

L'articolo 7, paragrafo 2, concerne le dichiarazioni scritte di consenso preformulate che riguardano anche altre questioni. Quando il consenso viene richiesto nell'ambito di un contratto (cartaceo), la richiesta di consenso deve essere chiaramente distinguibile dal resto. Se il contratto cartaceo tratta numerosi aspetti che non sono collegati al consenso all'uso dei dati personali, quest'ultimo deve essere trattato in modo da distinguersi chiaramente oppure in un documento distinto. Analogamente, ai sensi del considerando 32[39], se il consenso viene richiesto per via elettronica, la richiesta di consenso deve essere separata e distinta, e non può semplicemente figurare in un paragrafo all'interno delle condizioni generali di contratto/servizio. Per tener conto degli schermi di piccole dimensioni o degli spazi ristretti per le informazioni, può essere appro-

priata, se del caso, una modalità di visualizzazione delle informazioni "a livelli" per evitare eccessivi disturbi all'esperienza dell'utente o alla progettazione del prodotto.

Per rispettare il regolamento il titolare del trattamento che si basa sul consenso dell'interessato deve adempiere anche gli obblighi di informazione separati di cui agli articoli 13 e 14. Nella pratica il rispetto degli obblighi di informazione e del requisito del consenso informato possono portare in molti casi a un approccio integrato. Tuttavia la presente sezione è scritta nella consapevolezza che possa sussistere un consenso "informato" valido anche quando non tutti gli aspetti di cui agli articoli 13 e/o 14 sono menzionati nel processo di ottenimento del consenso (questi punti dovrebbero ovviamente essere menzionati altrove, come ad esempio nell'informativa sulla protezione dei dati personali dell'azienda). Il Gruppo di lavoro ha emanato linee guida separate sul requisito della trasparenza.

[Esempio 12]
L'azienda X è un titolare del trattamento che ha ricevuto reclami per il fatto che agli interessati non è chiaro l'uso dei dati per il quale si chiede loro il consenso. L'azienda ritiene quindi sia necessario verificare se le informazioni contenute nella sua richiesta di consenso sono comprensibili per gli interessati. X organizza gruppi di prova volontari di categorie specifiche dei propri clienti e presenta loro nuovi aggiornamenti delle informazioni di consenso prima di comunicarle esternamente. La selezione di tale gruppo rispetta il principio di indipendenza ed avviene sulla base di norme che garantiscono un risultato rappresentativo e non distorto. Il gruppo riceve un questionario e indica cosa ha capito delle informazioni e quale valutazione darebbe sulla comprensibilità e pertinenza delle informazioni. Il titolare del trattamento continua a eseguire prove fino a quando i gruppi di prova non indicano che le informazioni sono comprensibili. X redige una relazione della prova e la tiene disponibile per riferimento futuro. Questo esempio mostra un modo con cui X può dimostrare che gli interessati hanno ricevuto informazioni chiare prima di acconsentire al trattamento dei loro dati personali da parte di X.

[Esempio 13]
Un'azienda effettua un trattamento di dati basandosi sul presupposto del consenso. L'azienda utilizza un'informativa sulla protezione dei dati a più livelli che include una richiesta di consenso. L'azienda comunica tutti i dettagli di base del titolare del trattamento e le attività di trattamento dei dati previste[40]*. Tuttavia, l'azienda non indica in che modo sia possibile contattare il responsabile della protezione dei dati nel primo livello di informazioni dell'informativa. Ai fini della base legittima e valida per il trattamento ai sensi dell'articolo 6, questo titolare del trattamento ha ottenuto un consenso "informato" valido, anche se i dati di contatto del responsabile della protezione dei dati non sono stati comunicati all'interessato (nel primo livello di informazioni), a norma dell'articolo 13, paragrafo 1, lettera b) o dell'articolo 14, paragrafo 1, lettera b).*

3.4. MANIFESTAZIONE DI VOLONTÀ INEQUIVOCABILE

Il regolamento generale sulla protezione dei dati afferma chiaramente che il consenso richiede una dichiarazione o un'azione positiva inequivocabile da parte dell'interessato, il che significa che il consenso deve sempre essere espresso attraverso una dichiarazione o in modo attivo. Deve essere ovvio che l'interessato ha acconsentito al particolare trattamento.

L'articolo 2, lettera h), della direttiva 95/46/CE definisce il consenso come una "manifestazione di volontà con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento". L'articolo 4, punto 11, del regolamento generale sulla protezione dei dati si basa su tale definizione, chiarendo che il consenso, per essere valido, richiede una manifestazione *inequivocabile* mediante una *dichiarazione o azione positiva inequivocabile*, in conformità alle precedenti linee guida del Gruppo di lavoro.

Con "azione positiva inequivocabile" si intende che l'interessato deve aver intrapreso un'azione deliberata per acconsentire al trattamento specifico[41]. Il considerando 32 stabilisce ulteriori orientamenti al riguardo. Il consenso può essere raccolto attraverso una dichiarazione scritta o verbale (registrata), anche tramite mezzi elettronici.

Probabilmente il modo più rigoroso per soddisfare il criterio della "dichiarazione scritta" consiste nell'assicurarsi che l'interessato scriva una lettera o un messaggio di posta elettronica al titolare del trattamento spiegando ciò a cui acconsente esattamente. Tuttavia, spesso ciò non è realistico. Le dichiarazioni scritte possono avere forme e formati diversi che potrebbero essere conformi al regolamento generale sulla protezione dei dati.

Fatto salvo il diritto contrattuale (nazionale) in vigore, il consenso può essere ottenuto attraverso una dichiarazione verbale registrata, sebbene sia necessario prendere debita nota delle informazioni rese disponibili all'interessato prima dell'espressione del consenso. L'uso di caselle di adesione preselezionate non è valido ai sensi del regolamento. Il silenzio o l'inattività da parte dell'interessato, così come il semplice procedere all'uso di un servizio, non possono essere considerati una manifestazione attiva di scelta.

> ***[Esempio 14]***
> *Durante l'installazione di un software, l'applicazione richiede all'interessato di acconsentire a utilizzare segnalazioni di arresto anomalo non anonimizzate per migliorare il software. La richiesta di consenso è accompagnata da una informativa sulla protezione dei dati a più livelli che fornisce le necessarie informazioni. Selezionando attivamente la casella facoltativa "Acconsento", l'utente è in grado di eseguire validamente una "azione positiva inequivocabile" per acconsentire al trattamento.*

Il titolare del trattamento deve inoltre fare attenzione al fatto che il consenso non può essere ottenuto tramite la stessa azione con cui si accetta un contratto

o le condizioni generali di servizio. L'accettazione globale delle condizioni generali di contratto/servizio non può essere considerata come un'azione positiva inequivocabile ai fini del consenso all'uso dei dati personali. Il regolamento generale sulla protezione dei dati non consente al titolare del trattamento di mettere a disposizione caselle preselezionate o procedure di rinuncia (opt-out) che richiedono un intervento dell'interessato per rifiutare il consenso (ad esempio "caselle di rinuncia")[42].

Quando il consenso deve essere prestato a fronte di una richiesta elettronica, quest'ultima non deve interferire inutilmente con l'utilizzo del servizio per il quale viene fornito il consenso[43]. Un'azione positiva con cui l'interessato manifesta il proprio consenso può essere necessaria quando una modalità di espressione del consenso meno in violazione e meno invasiva potrebbe determinare ambiguità. Di conseguenza potrebbe essere necessario che, per essere efficace, la richiesta di consenso interrompa in una certa misura l'esperienza d'uso.

Tuttavia, nel contesto dei requisiti di cui al regolamento generale sulla protezione dei dati, il titolare del trattamento è libero di sviluppare un flusso di consenso adatto alla propria organizzazione. A inequivocabile in conformità con il regolamento.

Il titolare del trattamento dovrebbe progettare meccanismi di consenso che operano in maniera chiara per gli interessati. Il titolare del trattamento deve evitare ambiguità e garantire che l'azione con cui viene espresso il consenso possa essere distinta da altre azioni. La semplice prosecuzione dell'uso normale di un sito web non è pertanto un comportamento dal quale si può dedurre una manifestazione di volontà dell'interessato a prestare il consenso a un trattamento proposto.

[Esempio 15]
Far scorrere una barra su uno schermo, muovere la mano davanti a una telecamera intelligente, ruotare lo smartphone in senso orario o fargli compiere un movimento a otto potrebbero essere opzioni per indicare un consenso a patto che siano fornite informazioni chiare e sia inequivocabile che l'azione richiesta implica un consenso a una richiesta specifica (istruzione esemplificativa: se fai scorrere questa barra verso sinistra, acconsenti all'uso delle informazioni X per la finalità Y. Ripeti il movimento per confermare). Il titolare del trattamento deve essere in grado di dimostrare che il consenso è stato ottenuto in questo modo e l'interessato deve poter revocare il consenso con la stessa facilità con cui lo ha espresso.

[Esempio 16]
Scorrere un sito verso il basso o sfogliarne le pagine non sono azioni chiare e positive, poiché l'avviso che continuare a scorrere il sito costituirà un'espressione di consenso può essere difficile da distinguere e/o può essere trascurato inavvertitamente quando l'interessato scorre rapidamente grandi quantità di testo; inoltre tali azioni non sono sufficientemente inequivocabili.

Nel contesto digitale molti servizi necessitano di dati personali per funzionare, quindi gli interessati ricevono quotidianamente molteplici richieste di consenso che implicano risposte tramite clic e scorrimenti. Ne può derivare un certo grado di stanchezza a cliccare: se occorre farlo troppe volte, l'effettivo effetto di avvertimento dei meccanismi di consenso diminuisce.

Si può quindi verificare la situazione in cui le domande di consenso non vengono più lette, con un conseguente rischio specifico per l'interessato, in quanto in genere viene richiesto il consenso per azioni che in linea di principio sono illecite in assenza di consenso. Il regolamento generale sulla protezione dei dati impone al titolare del trattamento l'obbligo di sviluppare soluzioni per affrontare questo problema.

Un esempio spesso citato nel contesto online è l'ottenimento del consenso dell'utente di Internet tramite le impostazioni del browser. Tali impostazioni dovrebbero essere sviluppate in linea con le condizioni per la validità del consenso previste dal regolamento, come ad esempio il fatto che il consenso deve essere granulare per ciascuna delle finalità previste e che le informazioni da fornire per ottenere il consenso devono indicare i titolari del trattamento.

In ogni caso, il consenso deve sempre essere ottenuto prima che il titolare del trattamento inizi a trattare i dati personali per i quali è necessario il consenso. Il Gruppo di lavoro ha costantemente affermato nei precedenti pareri che il consenso dovrebbe essere espresso prima dell'avvio dell'attività di trattamento[44]. Sebbene il regolamento non prescriva esplicitamente all'articolo 4, punto 11, che il consenso debba essere manifestato prima dell'attività di trattamento, ciò è chiaramente implicito. La rubrica dell'articolo 6 e il verbo "ha espresso" di cui all'articolo 6, paragrafo 1, lettera a), confermano tale interpretazione. Consegue logicamente dall'articolo 6 e dal considerando 40 che prima di iniziare un trattamento dei dati deve sussistere una base legittima e valida. Pertanto, il consenso dovrebbe essere espresso prima che abbia luogo l'attività di trattamento. In linea di principio può essere sufficiente chiedere il consenso dell'interessato una sola volta. Tuttavia, il titolare del trattamento deve ottenere un nuovo consenso specifico qualora le finalità del trattamento dei dati cambino dopo che è stato ottenuto il consenso o qualora sia prevista una finalità aggiuntiva.

4. OTTENIMENTO DEL CONSENSO ESPLICITO

Il consenso esplicito è richiesto in talune circostanze nelle quali emergono gravi rischi per la protezione dei dati e in cui si ritiene quindi appropriato un livello elevato di controllo individuale sui dati personali. Il regolamento generale sulla protezione dei dati richiede il consenso esplicito all'articolo 9 per il trattamento di categorie particolari di dati, all'articolo 49[45] per i trasferimenti di dati verso paesi terzi od organizzazioni internazionali in assenza di garanzie adeguate, e all'articolo 22 per i processi decisionali automatizzati relativi alle persone fisiche, compresa la profilazione[46].

In base al regolamento, prerequisito per l'ottenimento di un consenso "conforme" è una "dichiarazione o un'azione positiva inequivocabile". Poiché il requisito del consenso "conforme" nel regolamento è già elevato a un livello superiore rispetto al requisito del consenso di cui alla direttiva 95/46/CE, è necessario chiarire quali sforzi supplementari debba attuare il titolare del trattamento per ottenere il consenso *esplicito* dell'interessato in linea con il regolamento.

Il termine *esplicito* si riferisce al modo in cui il consenso è espresso dall'interessato e significa che l'interessato deve fornire una dichiarazione esplicita di consenso. Un modo ovvio per assicurarsi che il consenso sia esplicito consisterebbe nel confermare espressamente il consenso in una dichiarazione scritta. Se del caso, il titolare del trattamento potrebbe assicurarsi che la dichiarazione potenziale mancanza di prove in futuro[47].

Tuttavia la dichiarazione firmata non è l'unico modo per ottenere il consenso esplicito e non si può affermare che il regolamento prescriva dichiarazioni scritte e firmate in tutte le circostanze che richiedono un consenso esplicito valido. Ad esempio, nel contesto digitale od online, l'interessato può emettere la dichiarazione richiesta compilando un modulo elettronico, inviando un'e-mail, caricando un documento scansionato con la propria firma oppure utilizzando una firma elettronica. In teoria, anche l'uso di dichiarazioni verbali può essere sufficientemente specifico per ottenere un consenso esplicito valido, tuttavia può essere difficile per il titolare del trattamento dimostrare che tutte le condizioni per la validità del consenso esplicito siano state soddisfatte quando la dichiarazione è stata registrata.

Un'organizzazione può anche ottenere il consenso esplicito tramite una conversazione telefonica, a condizione che le informazioni sulla scelta siano corrette, intelligibili e chiare e che venga richiesta una conferma specifica da parte dell'interessato (ad esempio premendo un pulsante o fornendo una conferma verbale).

[Esempio 17]
Il titolare del trattamento può ottenere il consenso esplicito da un visitatore del proprio sito web mettendo a disposizione una schermata di consenso esplicito contenente caselle di controllo "Sì" e "No", a condizione che il testo indichi chiaramente il consenso, ad esempio con una dicitura del tipo "In questo modo acconsento al trattamento dei miei dati" e non ad esempio tramite una formulazione del tipo "Mi è chiaro che i miei dati saranno trattati". Va da sé che devono essere soddisfatte le condizioni per il consenso informato e le altre condizioni per la validità del consenso.

[Esempio 18]
Una clinica per chirurgia estetica chiede il consenso esplicito di un paziente al trasferimento della cartella clinica a un esperto per un secondo parere sulla condizione del paziente. La cartella clinica è costituita da un file digitale. Data la natura specifica delle informazioni in questione, la clinica chiede la firma elettroni-

ca dell'interessato per ottenere un consenso esplicito valido e per essere in grado di dimostrare che è stato ottenuto detto consenso esplicito[48].

Anche la verifica in due fasi del consenso può essere un modo per assicurarsi che il consenso esplicito sia valido. Ad esempio, l'interessato riceve un'e-mail che gli notifica l'intenzione del titolare del trattamento di trattare una cartella contenente dati medici. Il titolare del trattamento spiega nell'e-mail che chiede il consenso all'uso di un insieme specifico di informazioni per una finalità specifica. Se l'interessato acconsente all'utilizzo dei dati, il titolare del trattamento gli chiede una risposta via e-mail contenente la dichiarazione "Acconsento". Dopo l'invio della risposta, l'interessato riceve un link di verifica da cliccare oppure un messaggio SMS con un codice di verifica, in maniera da confermare il consenso.

L'articolo 9, paragrafo 2, non riconosce il trattamento "necessario all'esecuzione di un contratto" come un'eccezione al divieto generale di trattare categorie particolari di dati. Di conseguenza i titolari del trattamento e gli Stati membri che rientrano nel contesto di applicazione di tale circostanza dovrebbero esaminare le eccezioni specifiche di cui all'articolo 9, paragrafo 2, lettere da b) a j). Qualora non si applichi nessuna delle eccezioni da b) a j), l'ottenimento del consenso esplicito in conformità con le condizioni per il consenso valido previste dal regolamento rimane l'unica eccezione lecita possibile per trattare tali dati.

[Esempio 19]
La compagnia aerea Holiday Airways offre un servizio di assistenza di viaggio ai passeggeri che non possono viaggiare senza assistenza, ad esempio a causa di una disabilità. Un cliente prenota un volo da Amsterdam a Budapest e richiede l'assistenza di viaggio per salire a bordo dell'aereo. Holiday Airways richiede al passeggero di fornire informazioni sulle sue condizioni di salute per essere in grado di organizzare i servizi appropriati (ad esempio, una sedia a rotelle a disposizione alla porta di imbarco o un assistente che viaggi con il passeggero da A a B). Holiday Airways richiede il consenso esplicito per trattare i dati sanitari del passeggero allo scopo di organizzare l'assistenza richiesta per il viaggio. I dati trattati sulla base del consenso devono essere necessari per il servizio richiesto. Inoltre i voli per Budapest sono disponibili anche senza assistenza di viaggio. Si noti che poiché tali dati sono necessari per la prestazione del servizio richiesto, l'articolo 7, paragrafo 4, non si applica.

[Esempio 20]
Un'azienda di successo è specializzata nella fornitura di occhiali da sci e da snowboard su misura e altri tipi di occhiali personalizzati per gli sport all'aria aperta. L'idea è che le persone possano indossare tali occhiali senza dover portare anche gli occhiali da vista. La società riceve ordini presso un punto centrale e consegna prodotti in tutta l'UE a partire da un'unica sede. Per poter fornire i propri prodotti personalizzati ai clienti miopi, tale titolare del trattamento richiede il consenso all'uso delle informazioni sulle condizioni di vista dei clienti. I clienti forniscono i dati sanitari necessari - ad esempio i dati della loro prescrizione - online quando effettuano l'ordine. Senza questi dati non sarebbe possibile fornire gli oc-

chiali personalizzati richiesti. L'azienda offre anche una serie di occhiali con valori correttivi standardizzati. I clienti che non desiderano condividere i dati sanitari possono optare quindi per le versioni standard. Di conseguenza, nel caso di specie, è richiesto un consenso esplicito ai sensi dell'articolo 9 e il consenso può essere considerato come espresso liberamente.

5. CONDIZIONI AGGIUNTIVE PER L'OTTENIMENTO DI UN CONSENSO VALIDO

Il regolamento generale sulla protezione dei dati introduce requisiti che impongono al titolare del trattamento di prevedere modalità aggiuntive per garantire che ottiene un consenso valido, lo mantiene e sia in grado di dimostrarne l'esistenza. L'articolo 7 del stabilisce queste condizioni aggiuntive per il consenso valido tramite disposizioni specifiche sulla conservazione di registrazioni del consenso e sul diritto di revocare facilmente il consenso espresso. L'articolo 7 si applica anche al consenso di cui ad altri articoli del regolamento, ad esempio gli articoli 8 e 9. Si riportano in appresso orientamenti sull'ulteriore requisito di dimostrare l'esistenza di un consenso valido e sulla revoca del consenso.

5.1. DIMOSTRAZIONE DEL CONSENSO

L'articolo 7, paragrafo 1, prevede in maniera chiara l'obbligo esplicito del titolare del trattamento di dimostrare il consenso dell'interessato. Conformemente a tale articolo, l'onere della prova è a carico del titolare del trattamento. Il considerando 42 afferma: *"Per i trattamenti basati sul consenso dell'interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento"*.

Il titolare del trattamento è libero di sviluppare metodi propri per rispettare tale disposizione in maniera adatta alle sue attività quotidiane. Allo stesso tempo, l'obbligo in capo al titolare del trattamento di dimostrare l'ottenimento di un consenso valido non dovrebbe di per sé portare a quantità eccessive di trattamenti di dati supplementari. Ciò significa che il titolare del trattamento dovrebbe disporre di dati sufficienti per mostrare un collegamento al trattamento (ossia per fornire la prova che è stato ottenuto il consenso) ma non dovrebbe raccogliere più informazioni di quanto necessario.

Spetta al titolare del trattamento dimostrare che è stato ottenuto un consenso valido dall'interessato. Il regolamento non prescrive esattamente come ciò debba avvenire. Tuttavia, il titolare del trattamento deve essere in grado di dimostrare che l'interessato nel caso specifico ha espresso il proprio consenso. Fintantoché dura l'attività di trattamento dei dati in questione, sussiste l'obbligo di dimostrare l'esistenza del consenso. Al termine dell'attività di trattamento, la prova del consenso deve essere conservata non più di quanto strettamente necessario per adempiere ad obblighi giuridici o per l'accertamento,

l'esercizio o la difesa di un diritto in sede giudiziaria, in conformità con l'articolo 17, paragrafo 3, lettere b) ed e).

Ad esempio, il titolare del trattamento può tenere una registrazione delle dichiarazioni di consenso ricevute onde poter dimostrare come e quando è stato ottenuto il consenso, e rendere dimostrabili le informazioni fornite all'interessato al momento dell'espressione del consenso. Il titolare del trattamento deve anche essere in grado di dimostrare che l'interessato è stato informato e che la propria procedura ha soddisfatto tutti i criteri pertinenti per la validità del consenso. La logica alla base di tale obbligo è che il titolare del trattamento deve essere responsabilizzato in relazione all'ottenimento di un consenso valido dell'interessato e ai meccanismi di consenso che ha messo in atto. Ad esempio, in un contesto online, il titolare del trattamento può conservare informazioni sulla sessione in cui è stato espresso il consenso, unitamente alla documentazione della procedura di consenso al momento della sessione, oltre a una copia delle informazioni presentate all'interessato in quel momento. Non sarebbe sufficiente fare semplicemente riferimento a una corretta configurazione del sito web.

> ***[Esempio 21]***
> *Un ospedale istituisce un programma di ricerca scientifica per il quale sono necessarie cartelle cliniche odontoiatriche di pazienti. I partecipanti sono selezionati tramite telefonate a pazienti che hanno volontariamente accettato di essere inseriti in un elenco di candidati che possono essere contattati a tale fine. Il titolare del trattamento chiede il consenso esplicito degli interessati all'uso della loro cartella clinica odontoiatrica. Il consenso viene ottenuto durante una telefonata, registrando una dichiarazione verbale dell'interessato nella quale quest'ultimo conferma di acconsentire all'uso dei suoi dati per le finalità del programma.*

Il regolamento non specifica alcun termine per la durata del consenso. Questa dipenderà dal contesto, dalla portata del consenso originale e dalle aspettative dell'interessato. Se i trattamenti cambiano o si evolvono in maniera considerevole, il consenso originale non è più valido e occorrerà un nuovo consenso.

Come migliore prassi il Gruppo di lavoro raccomanda di aggiornare il consenso a intervalli appropriati. Fornire nuovamente tutte le informazioni contribuisce a garantire che l'interessato rimanga ben informato su come vengono utilizzati i suoi dati e su come può esercitare i suoi diritti[49].

5.2. REVOCA DEL CONSENSO

Il regolamento generale sulla protezione dei dati dà ampio rilievo alla revoca del consenso. Le disposizioni e i considerando relativi alla revoca del consenso possono considerarsi una codificazione dell'interpretazione data al riguardo nei pareri del Gruppo di lavoro[50].

L'articolo 7, paragrafo 3, prescrive che il titolare del trattamento deve garantire che l'interessato possa revocare il consenso in qualsiasi momento con la stessa

facilità con cui lo ha espresso. Il regolamento non dispone che l'espressione e la revoca del consenso debbano avvenire sempre allo stesso modo.

Tuttavia, quando il consenso viene prestato per via elettronica con un solo clic di mouse, un solo scorrimento o premendo un tasto, l'interessato deve, in pratica, poterlo revocare con altrettanta facilità. Se il consenso è espresso attraverso un'interfaccia utente specifica di servizio (ad esempio un sito web, un'applicazione, un account protetto, l'interfaccia di un dispositivo IoT oppure posta elettronica), è indubbio che l'interessato deve poterlo revocare tramite la medesima interfaccia elettronica, poiché il passaggio a un'altra interfaccia per la sola revoca richiederebbe uno sforzo eccessivo. Inoltre, l'interessato dovrebbe poter revocare il consenso senza subire pregiudizio. Ciò significa, tra l'altro, che il titolare del trattamento deve consentire la revoca senza spese o senza abbassare i livelli del servizio[51].

> ***[Esempio 22]***
> *Un festival musicale vende biglietti tramite un agente di vendita di biglietti online. All'atto della vendita del biglietto viene richiesto il consenso all'uso dei dettagli di contatto per finalità di marketing. Per acconsentire o meno a tale finalità, il cliente può cliccare su "Sì" oppure su "No". Il titolare del trattamento informa il cliente che può revocare il consenso contattando gratuitamente un call center nei giorni lavorativi tra le 8:00 e le 17:00. Il titolare del trattamento di questo esempio non rispetta l'articolo 7, paragrafo 3, del regolamento. Telefonare durante l'orario di lavoro per revocare il consenso è più oneroso rispetto a un clic di mouse per prestare il consenso attraverso il venditore di biglietti online, che è aperto 24 ore al giorno, 7 giorni la settimana.*

In base al regolamento il requisito della facilità della revoca è un elemento necessario del consenso valido. Se il diritto di revoca non soddisfa i requisiti del regolamento, il meccanismo di consenso del titolare del trattamento non è conforme al regolamento. Come menzionato nella sezione 3.1 sulla condizione del consenso informato, a norma dell'articolo 7, paragrafo 3, del regolamento il titolare del trattamento deve informare l'interessato del diritto di revoca prima che quest'ultimo presti effettivamente il consenso. Inoltre, nel contesto dell'obbligo di trasparenza, il titolare del trattamento deve informare l'interessato sulle modalità di esercizio dei suoi diritti[52].

Di norma, se il consenso viene revocato, tutti i trattamenti dei dati basati sul consenso avvenuti prima della revoca (e in conformità con il regolamento) rimangono leciti, tuttavia il titolare del trattamento deve interrompere le attività di trattamento interessate. Qualora non sussista un'altra base legittima per il trattamento (ad esempio l'ulteriore archiviazione) dei dati, questi dovrebbero essere cancellati dal titolare del trattamento[53].

Come già accennato, prima di raccogliere i dati è molto importante che il titolare del trattamento valuti le finalità per le quali i dati sono effettivamente trattati e le basi legittime del trattamento. Spesso le aziende hanno bisogno di dati personali per diverse finalità e il trattamento si basa su più basi legittime,

ad esempio il trattamento di dati dei clienti può basarsi su un contratto e sul consenso. Di conseguenza, la revoca del consenso non implica che il titolare del trattamento deve cancellare i dati trattati per una finalità che si basa sull'esecuzione del contratto stipulato con l'interessato. Il titolare del trattamento dovrebbe pertanto precisare chiaramente sin dall'inizio la finalità che si applica a ciascun dato e le basi legittime del trattamento.

Il titolare del trattamento deve cancellare i dati trattati sulla base del consenso non appena questo viene revocato, supponendo che non vi siano altre finalità che giustificano l'ulteriore conservazione[54].
Oltre a questa situazione, prevista dall'articolo 17, paragrafo 1, lettera b), l'interessato può chiedere la cancellazione di altri dati che lo riguardano trattati sulla base di un'altra base legittima, ad esempio l'articolo 6, paragrafo 1, lettera b)[55]. Il titolare del trattamento è tenuto a valutare se la prosecuzione del trattamento dei dati in questione sia appropriata, anche in assenza di una richiesta di cancellazione da parte dell'interessato[56].

In caso di revoca del consenso, il titolare del trattamento, se vuole continuare a trattare i dati personali in base a un'altra base legittima, non può passare tacitamente dal consenso (che è stato revocato) all'altra base legittima. Qualsiasi modifica della base legittima del trattamento deve essere notificata all'interessato in conformità ai requisiti di informazione di cui agli articoli 13 e 14, nonché al principio generale di trasparenza.

6. INTERAZIONE TRA IL CONSENSO E ALTRE BASI LEGITTIME DI CUI ALL'ARTICOLO 6 DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

L'articolo 6 stabilisce le condizioni per la liceità del trattamento dei dati personali ed elenca sei basi legittime su cui il titolare del trattamento può fondarsi. L'applicazione di una di queste sei basi deve essere stabilita prima di procedere al trattamento e in relazione a una finalità specifica[57].

È importante osservare che, se sceglie di basarsi sul consenso per ogni parte del trattamento, il titolare del trattamento deve essere preparato a rispettare tale scelta e interrompere la parte del trattamento in caso di revoca del consenso. Comunicare che i dati saranno trattati sulla base del consenso mentre in realtà si fa affidamento su un'altra base legittima sarebbe fondamentalmente scorretto nei confronti dell'interessato.

In altre parole, il titolare del trattamento non può passare dal consenso ad altre basi legittime. Ad esempio non può ricorrere retroattivamente alla base dell'interesse legittimo in caso di problemi di validità del consenso. Poiché ha l'obbligo di comunicare la base legittima al momento della raccolta dei dati personali, il titolare del trattamento deve aver deciso la base legittima prima della raccolta dei dati.

7. SETTORI SPECIFICI DI INTERESSE NEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

7.1. MINORI (ARTICOLO 8)

Rispetto alla direttiva attuale, il regolamento generale sulla protezione dei dati crea un ulteriore livello di protezione per il trattamento dei dati personali delle persone fisiche vulnerabili, in particolare i minori. L'articolo 8 introduce obblighi supplementari per garantire una maggiore protezione dei dati dei minori in relazione ai servizi della società dell'informazione. I motivi di tale protezione rafforzata sono specificati nel considerando 38: *"I minori [...] possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali [...]". Sempre al considerando 38 si afferma che "[t]ale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore"*. La precisazione "in particolare" indica che la protezione specifica non si limita al marketing o alla profilazione, ma si estende alla più ampia "raccolta di dati personali relativi ai minori".

L'articolo 8, paragrafo 1, stabilisce che laddove si applichi il consenso, per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui il consenso è prestato o autorizzato dal titolare della responsabilità genitoriale[58]. Per quanto concerne il limite di età per il consenso valido, il regolamento offre flessibilità, in quanto gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

Come menzionato nella sezione 3.1. sul consenso informato, le informazioni fornite dal titolare del trattamento devono essere comprensibili per il pubblico al quale sono destinate, con particolare attenzione alla posizione dei minori. Per ottenere il "consenso informato" di un minore, il titolare del trattamento deve spiegare in un linguaggio chiaro e semplice, comprensibile per i minori, come intende trattare i dati raccolti[59]. Se spetta al genitore prestare il consenso, può essere necessario fornire un insieme di informazioni che consentano agli adulti di prendere una decisione informata.

Da quanto precede risulta evidente che l'articolo 8 si applica esclusivamente quando sono soddisfatte le seguenti condizioni:

- il trattamento è correlato all'offerta diretta di servizi della società dell'informazione ai minori[60,61];
- il trattamento è basato sul consenso.

7.1.1. SERVIZIO DELLA SOCIETÀ DELL'INFORMAZIONE

Al fine di determinare la portata dell'espressione "servizio della società dell'informazione", il regolamento generale sulla protezione dei dati, all'articolo 4, punto 25, fa riferimento alla direttiva (UE) 2015/1535.

Per valutare la portata di tale definizione, il Gruppo di lavoro fa riferimento anche alla giurisprudenza della Corte di giustizia[62]. La Corte di giustizia ha affermato che la nozione di *servizi della società dell'informazione* interessa contratti e altri servizi conclusi o trasmessi online.

Laddove un servizio presenti due componenti economicamente indipendenti, una delle quali è la componente online (ad esempio l'offerta e l'accettazione di un'offerta nel contesto della conclusione di un contratto, o le informazioni relative a prodotti o servizi, comprese le attività di marketing) e l'altra è la consegna fisica o la distribuzione di merci, la prima rientra nella definizione di servizio della società dell'informazione, mentre la seconda no. La consegna online di un servizio rientrerebbe nell'espressione servizio della società dell'informazione di cui all'articolo 8 del regolamento generale sulla protezione dei dati.

7.1.2. FORNITI DIRETTAMENTE A UN MINORE

La precisazione "offerta diretta [...] ai minori" indica che l'articolo 8 si applica ad alcuni ma non a tutti i servizi della società dell'informazione. A tale riguardo, se un prestatore di servizi della società dell'informazione chiarisce ai potenziali utenti che il servizio è offerto esclusivamente a persone aventi almeno 18 anni, e ciò non è smentito da altri elementi (come il contenuto del sito o piani di marketing), allora il servizio non sarà considerato fornito direttamente a un minore e l'articolo 8 non si applicherà.

7.1.3. ETÀ

Il regolamento specifica che *"[g]li Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni"*. Nel tenere conto del pubblico destinatario dei suoi servizi, il titolare del trattamento deve tenere presenti le diverse leggi nazionali. In particolare, il titolare del trattamento che fornisce un servizio transfrontaliero non può sempre fare affidamento sul solo rispetto della legge dello Stato membro in cui ha lo stabilimento principale, perché potrebbe dover rispettare le leggi nazionali di ciascuno Stato membro in cui offre i servizi della società dell'informazione, a seconda che lo Stato membro scelga di usare come criterio di legge il luogo dello stabilimento principale del titolare del trattamento oppure il luogo di residenza dell'interessato. Nello scegliere il criterio da usare gli Stati membri devono considerare innanzitutto l'interesse superiore del minore. Il Gruppo di lavoro incoraggia gli Stati membri a cercare una soluzione armonizzata.

Nel fornire servizi della società dell'informazione ai minori sulla base del consenso, il titolare del trattamento dovrà compiere ogni ragionevole sforzo per verificare che l'utente abbia raggiunto l'età del consenso digitale, e le misure dovrebbero essere proporzionate alla natura e ai rischi delle attività di trattamento.

Se l'utente afferma di aver raggiunto l'età del consenso digitale, il titolare del trattamento può effettuare controlli appropriati per verificare la veridicità della dichiarazione. Sebbene il regolamento non richieda esplicitamente di intraprendere sforzi ragionevoli per verificare l'età, tale necessità è implicita, poiché se un minore presta il consenso senza avere l'età sufficiente per prestare un consenso valido per proprio conto il trattamento dei dati sarà illecito.

Se l'utente dichiara di avere un'età inferiore a quella del consenso digitale, il titolare del trattamento può accettare tale dichiarazione senza ulteriori verifiche, ma dovrà ottenere l'autorizzazione dei genitori e verificare che la persona che esprime il consenso sia titolare della responsabilità genitoriale.

La verifica dell'età non deve comportare un eccessivo trattamento di dati. Il meccanismo scelto per verificare l'età dell'interessato dovrebbe prevedere una valutazione del rischio del trattamento proposto. In alcune situazioni a basso rischio, potrebbe essere adeguato richiedere al nuovo abbonato al servizio di rivelare il proprio anno di nascita oppure di compilare un modulo in cui dichiara di (non) essere un minore[63]. Qualora dovessero sorgere dubbi, il titolare del trattamento dovrebbe riesaminare i meccanismi di verifica dell'età nel caso di specie e valutare se siano necessari controlli alternativi[64].

7.1.4. CONSENSO DEL MINORE E RESPONSABILITÀ GENITORIALE

Per quanto riguarda l'autorizzazione del titolare della responsabilità genitoriale, il regolamento non prevede modalità pratiche per raccogliere il consenso del genitore o per stabilire che qualcuno è autorizzato a prestare il consenso[65]. Di conseguenza il Gruppo di lavoro raccomanda l'adozione di un approccio proporzionato, in linea con l'articolo 8, paragrafo 2, e l'articolo 5, paragrafo 1, lettera c), del regolamento (minimizzazione dei dati). Un approccio proporzionato potrebbe essere quello di concentrarsi sull'ottenimento di una quantità limitata di informazioni, ad esempio i dettagli di contatto di un genitore o del tutore.

La ragionevolezza degli sforzi, in termini di verifica tanto che l'utente abbia l'età sufficiente per esprimere il consenso quanto che la persona che esprime il consenso a nome del minore sia il titolare della responsabilità genitoriale, può dipendere dai rischi inerenti al trattamento e dalla tecnologia disponibile. Nei casi a basso rischio, può essere sufficiente la verifica della responsabilità genitoriale a mezzo posta elettronica. Viceversa, nei casi ad alto rischio, può essere opportuno chiedere ulteriori prove affinché il titolare del trattamento sia in grado di verificare e conservare le informazioni di cui all'articolo 7, paragrafo

1[66]. I servizi di verifica di terzi fidati possono offrire soluzioni che riducono al minimo la quantità di dati personali che il titolare del trattamento deve trattare autonomamente.

> ***[Esempio 23]***
> *Una piattaforma di gioco online vuole assicurarsi che i clienti minorenni si abbonino ai servizi esclusivamente con il consenso dei genitori o tutori. Il titolare del trattamento segue questi passaggi:*
> *passaggio 1: chiede all'utente di indicare se ha meno o più di 16 anni (o dell'età alternativa per il consenso digitale).*
> *Se l'utente dichiara di avere un'età inferiore a quella per il consenso digitale:*
> *passaggio 2: il servizio informa il minore della necessità che un genitore o il tutore acconsenta o autorizzi il trattamento prima che venga erogato il servizio. All'utente viene quindi richiesto di rivelare l'indirizzo di posta elettronica di un genitore o del tutore;*
> *passaggio 3: il servizio contatta il genitore o il tutore e ne ottiene il consenso al trattamento tramite posta elettronica e adotta misure ragionevoli per ottenere la conferma che l'adulto abbia la responsabilità genitoriale; passaggio 4: in caso di reclami, la piattaforma adotta ulteriori provvedimenti per verificare l'età dell'abbonato. Se soddisfa gli altri requisiti del consenso, la piattaforma può soddisfare i criteri supplementari di cui all'articolo 8 del regolamento seguendo questi passaggi.*

L'esempio mostra che il titolare del trattamento può mettersi in una posizione tale da dimostrare che sono stati compiuti sforzi ragionevoli per garantire che è stato ottenuto un consenso valido in relazione ai servizi forniti a un minore. L'articolo 8, paragrafo 2, aggiunge in particolare che "[i]l titolare del trattamento si adopera in ogni modo ragionevole per verificare che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili".

Spetta al titolare del trattamento stabilire quali misure siano appropriate in un caso specifico. Di norma, il titolare del trattamento dovrebbe evitare soluzioni di verifica che implichino una raccolta eccessiva di dati personali.

Il Gruppo di lavoro riconosce che in determinati casi la verifica è difficile, ad esempio se il minore che presta il consenso non ha ancora lasciato un'"impronta di identità" o se la responsabilità genitoriale non è facilmente verificabile. Tale aspetto può essere preso in considerazione nel decidere quali sforzi siano ragionevoli, tuttavia ci si aspetta anche che il titolare del trattamento tenga sotto costante controllo i suoi processi e la tecnologia disponibile.

Per quanto riguarda l'autonomia dell'interessato a manifestare il consenso al trattamento dei dati personali e il pieno controllo sul trattamento, nel momento in cui raggiunge l'età del consenso digitale l'interessato può confermare, modificare o revocare il consenso prestato o autorizzato dal titolare della responsabilità genitoriale.

In pratica, ciò significa che se il minore non intraprende alcuna azione, il consenso prestato o autorizzato dal titolare della responsabilità genitoriale in relazione al trattamento dei dati personali forniti prima dell'età del consenso digitale rimarrà un presupposto valido per il trattamento.

Una volta raggiunta l'età del consenso digitale, il minore avrà la possibilità di revocare il consenso, in linea con l'articolo 7, paragrafo 3. In conformità con i principi di correttezza e responsabilizzazione, il titolare del trattamento deve informare il minore di questa possibilità[67].

È importante sottolineare che, ai sensi del considerando 38, il consenso di un genitore o del tutore non è richiesto nel contesto di servizi di prevenzione o consulenza offerti direttamente al minore. Ad esempio, per i servizi di protezione dei minori offerti online ai minori tramite un servizio di chat non occorre la previa autorizzazione dei genitori.

Infine, il regolamento prevede che le norme relative ai requisiti di autorizzazione genitoriale nei confronti dei minori non pregiudicano "le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore". Di conseguenza i requisiti per la validità del consenso all'uso dei dati relativi a minori rientrano in un quadro giuridico da considerarsi distinto dal diritto contrattuale nazionale. Le presenti linee guida non affrontano pertanto la questione se sia lecito o meno per un minore concludere contratti online. Entrambi i regimi giuridici possono essere applicati simultaneamente e l'ambito di applicazione del regolamento generale sulla protezione dei dati non include l'armonizzazione delle disposizioni nazionali di diritto contrattuale.

7.2. RICERCA SCIENTIFICA

La definizione di finalità di ricerca scientifica ha implicazioni sostanziali per la gamma di attività di trattamento di dati che un titolare del trattamento può intraprendere. L'espressione "ricerca scientifica" non è definita nel regolamento. Il considerando 159 afferma: "*[...] Nell'ambito del presente regolamento, il trattamento di dati personali per finalità di ricerca scientifica dovrebbe essere interpretato in senso lato. [...]*", tuttavia il Gruppo di lavoro ritiene che tale nozione non possa essere estesa oltre il suo significato comune e che per "ricerca scientifica" in questo contesto si intenda un progetto di ricerca istituito in conformità con le pertinenti norme metodologiche e deontologiche settoriali, in linea con le buone prassi.

Quando il consenso costituisce la base legittima per condurre ricerche in conformità con il regolamento, tale consenso all'uso dei dati personali dovrebbe essere distinto dagli altri requisiti del consenso che fungono da norme deontologiche od obbligo procedurale. Un esempio di obbligo procedurale, in cui il trattamento si basa non sul consenso ma su un'altra base giuridica, figura nel regolamento sulla sperimentazione clinica. Nel contesto del diritto in materia

di protezione dei dati, quest'ultima forma di consenso potrebbe essere considerata una garanzia aggiuntiva[68]. Allo stesso tempo, il regolamento generale sulla protezione dei dati non limita l'applicazione dell'articolo 6 al solo consenso, per quanto riguarda il trattamento di dati per fini di ricerca. Fintantoché sussistono garanzie adeguate, quali i requisiti di cui all'articolo 89, paragrafo 1, e il trattamento è corretto, lecito, trasparente e conforme alle norme sulla minimizzazione dei dati e ai diritti individuali, potrebbero essere disponibili altre basi legittime quali l'articolo 6, paragrafo 1, lettera e) o f)[69]. Ciò vale anche per le categorie particolari di dati ai sensi della deroga di cui all'articolo 9, paragrafo 2, lettera j)[70].

Il considerando 33 sembra consentire una certa flessibilità al grado di specificazione e granularità del consenso nel contesto della ricerca scientifica. Esso afferma: *"In molti casi non è possibile individuare pienamente la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, dovrebbe essere consentito agli interessati di prestare il proprio consenso a taluni settori della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica. Gli interessati dovrebbero avere la possibilità di prestare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca nella misura consentita dalla finalità prevista"*.

In primo luogo, va osservato che il considerando 33 non inficia gli obblighi relativi al requisito del consenso specifico. Ciò significa che, in linea di principio, i progetti di ricerca scientifica possono includere dati personali sulla base del consenso soltanto se hanno una finalità ben descritta. Nei casi in cui le finalità del trattamento dei dati nell'ambito di un progetto di ricerca scientifica non possono essere specificate in via preliminare, il considerando 33 consente in via eccezionale che la finalità possa essere descritta a un livello più generale.

Tenuto conto delle condizioni rigorose stabilite dall'articolo 9 in merito al trattamento di categorie particolari di dati, il Gruppo di lavoro rileva che quando categorie particolari di dati vengono trattate sulla base del consenso esplicito, l'applicazione dell'approccio flessibile di cui al considerando 33 sarà soggetta a un'interpretazione più rigorosa e richiede un elevato livello di controllo.

Considerato nel suo insieme, il regolamento generale sulla protezione dei dati non può essere interpretato in maniera tale da consentire al titolare del trattamento di aggirare il principio chiave della specificazione delle finalità per le quali viene richiesto il consenso dell'interessato.

Quando non è possibile specificare appieno le finalità della ricerca, il titolare del trattamento deve cercare altri modi per garantire il rispetto dell'essenza dei requisiti del consenso, ad esempio permettendo agli interessati di acconsentire a una finalità di ricerca in termini più generali e a fasi specifiche di un progetto di ricerca che si sa già sin dall'inizio avranno luogo. Mano a mano che la ricerca avanza, sarà quindi possibile ottenere il consenso per le fasi successive del progetto prima dell'inizio della fase corrispondente. Tuttavia, tale consenso

dovrebbe comunque essere in linea con le norme deontologiche applicabili alla ricerca scientifica.

Inoltre, il titolare del trattamento può applicare ulteriori garanzie in questi casi. L'articolo 89, paragrafo 1, ad esempio, sottolinea la necessità di prevedere garanzie nelle attività di trattamento di dati per fini di ricerca scientifica o storica o per fini statistici. Tali finalità "*[sono] soggett[e] a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento*". Come possibili garanzie si menzionano la minimizzazione dei dati, l'anonimizzazione e la sicurezza dei dati[71]. L'anonimizzazione rappresenta la soluzione preferita non appena la finalità della ricerca possa essere conseguita senza il trattamento di dati personali.

La trasparenza è un'ulteriore garanzia quando le circostanze della ricerca non consentono un consenso specifico. La mancanza di specificazione della finalità può essere compensata dalla fornitura periodica, da parte del titolare del trattamento, di informazioni sullo sviluppo della finalità durante l'avanzamento del progetto di ricerca, in maniera tale che, nel tempo, il consenso sia il più specifico possibile. In tal modo l'interessato ha quanto meno una conoscenza di base dello stato di avanzamento, che gli consente di valutare se esercitare o meno, ad esempio, il diritto di revoca del consenso ai sensi dell'articolo 7, paragrafo 3[72].

Anche la messa a disposizione di un piano di ricerca esaustivo al quale gli interessati possano fare riferimento prima di esprimere il loro consenso potrebbe contribuire a compensare una mancanza di specificazione delle finalità[73]. Il piano di ricerca dovrebbe specificare nella maniera più chiara possibile i quesiti che la ricerca si pone e i metodi di lavoro previsti. Il piano di ricerca potrebbe altresì contribuire al rispetto dell'articolo 7, paragrafo 1, in quanto, per poter dimostrare che il consenso è valido, il titolare del trattamento è tenuto a dimostrare quali informazioni erano disponibili agli interessati al momento dell'espressione del consenso.

È importante ricordare che quando il consenso costituisce la base legittima del trattamento, l'interessato deve avere la possibilità di revocarlo. Il Gruppo di lavoro rileva che la revoca del consenso potrebbe compromettere taluni tipi di ricerca scientifica che richiedono dati che possano essere collegati a persone fisiche, tuttavia il regolamento è chiaro nello stabilire che il consenso può essere revocato e che il titolare del trattamento deve tenerne conto: non vi è alcuna esenzione a questo requisito per la ricerca scientifica. Se riceve una richiesta di revoca, il titolare del trattamento deve, in linea di principio, cancellare immediatamente i dati personali se vuole continuare a utilizzare i dati per le finalità della ricerca[74].

7.3. DIRITTI DELL'INTERESSATO

Se l'attività di trattamento di dati si basa sul consenso, i diritti dell'interessato subiscono alcune ripercussioni: l'interessato può avere il diritto alla portabilità

dei dati (articolo 20), ma non il diritto di opposizione (articolo 21), sebbene il diritto di revocare il consenso in qualsiasi momento possa portare a un esito analogo.

Gli articoli da 16 a 20 del regolamento generale sulla protezione dei dati indicano che (quando il trattamento dei dati è basato sul consenso) l'interessato ha il diritto alla cancellazione, in caso di revoca del consenso, e i diritti di limitazione del trattamento, rettifica e accesso[75].

8. CONSENSO OTTENUTO A NORMA DELLA DIRETTIVA 95/46/CE

I titolari del trattamento che attualmente trattano dati sulla base del consenso conformemente alla normativa nazionale in materia di protezione dei dati non sono automaticamente tenuti a rinnovare completamente tutte le relazioni di consenso con gli interessati in preparazione dell'entrata in vigore del regolamento generale sulla protezione dei dati. Il consenso ottenuto continua ad essere valido nella misura in cui è in linea con le condizioni stabilite nel regolamento generale sulla protezione dei dati.

È importante che prima del 25 maggio 2018 i titolari del trattamento rivedano in maniera approfondita i processi di lavoro e le registrazioni correnti, al fine di accertarsi che i consensi in essere soddisfino quanto previsto dal regolamento generale sulla protezione dei dati (cfr. considerando 171 del regolamento generale sulla protezione dei dati[76]). In pratica, il regolamento generale sulla protezione dei dati fissa prescrizioni più rigorose riguardo all'attuazione di meccanismi di consenso e introduce nuovi requisiti che impongono ai titolari del trattamento di modificare i meccanismi di consenso, non di riscrivere soltanto le politiche in materia di protezione dei dati[77].

Ad esempio, poiché il regolamento impone al titolare del trattamento di essere in grado di dimostrare che ha ottenuto un consenso valido, tutti i presunti consensi dei quali non viene conservato alcun riferimento si considereranno automaticamente al di sotto del livello di consenso fissato dal regolamento e dovranno quindi essere rinnovati. Analogamente, poiché il regolamento richiede una "dichiarazione o un'azione positiva inequivocabile", tutti i presunti consensi basati su una forma di azione più implicita dell'interessato (ad esempio una casella di adesione preselezionata) non saranno conformi al livello di consenso stabilito dal regolamento.

Inoltre, per poter dimostrare l'ottenimento del consenso o fornire indicazioni più granulari sulle volontà dell'interessato, il titolare del trattamento potrebbe dover effettuare un riesame delle operazioni e dei sistemi informativi. Devono essere disponibili meccanismi che consentano agli interessati di revocare facilmente il consenso e devono essere fornite informazioni su come revocare il consenso. Se le procedure esistenti per l'ottenimento e la gestione del consenso non soddisfano i livelli previsti dal regolamento, il titolare del trattamento dovrà ottenere un nuovo consenso conforme al regolamento.

D’altro canto, poiché non tutti gli elementi indicati negli articoli 13 e 14 devono sempre essere presenti come condizione per un consenso informato, gli obblighi di informazione estesa ai sensi del regolamento non si oppongono necessariamente alla continuità del consenso prestato prima dell’entrata in vigore del regolamento (cfr. precedente pagina 15). La direttiva 95/46/CE non prevedeva alcun obbligo di informare gli interessati in merito alla base del trattamento.

Qualora ritenga che il consenso ottenuto in base alla vecchia normativa non rispetti le norme per il consenso fissate dal regolamento, il titolare del trattamento deve agire per conformarvisi, ad esempio mediante il rinnovo del consenso in un maniera conforme al regolamento. Ai sensi del regolamento non è possibile passare da una base legittima a un’altra. Se il titolare del trattamento non è in grado di rinnovare il consenso in maniera conforme né è in grado, come circostanza una tantum, di conformarsi al regolamento basando il trattamento dei dati su una base legittima diversa garantendo nel contempo che la prosecuzione del trattamento corrisponda ai principi di correttezza e responsabilizzazione, le attività di trattamento devono essere interrotte. In ogni caso, il titolare del trattamento deve rispettare i principi di un trattamento lecito, corretto e trasparente.

NOTE

[1] L'articolo 9 del regolamento generale sulla protezione dei dati fornisce un elenco di possibili esenzioni al divieto di trattamento di categorie particolari di dati. Una delle esenzioni elencate è il consenso esplicito dell'interessato all'uso di tali dati.

[2] Cfr. anche il parere 15/2011 sulla definizione di consenso (WP 187), pagine 6-8 e/o il parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE (WP 217), pagg. 9, 10, 13 e 14.

[3] In particolare il parere 15/2011 sulla definizione di consenso (WP 187).

[4] Parere 15/2011 sulla definizione di consenso (WP 187), pag. 9.

[5] Cfr. anche il parere 15/2011 sulla definizione di consenso (WP 187) e l'articolo 5 del regolamento generale sulla protezione dei dati.

[6] Ai sensi dell'articolo 9 della proposta di regolamento sulla vita privata e le comunicazioni elettroniche, si applicano la definizione e le condizioni per il consenso di cui all'articolo 4, punto 11, e all'articolo 7, del regolamento generale sulla protezione dei dati.

[7] Cfr. *"Opinion 03/2016 on the evaluation and review of the ePrivacy Directive"* [Parere 03/2016 sulla valutazione e la revisione della direttiva relativa alla vita privata e alle comunicazioni elettroniche] (WP 240).

[8] Cfr. articolo 94 del regolamento generale sulla protezione dei dati.

[9] Il consenso, definito nella direttiva 95/46/CE come *"qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento"*, deve essere *"manifestato in maniera inequivocabile"* in maniera da rendere legittimo il trattamento dei dati personali (articolo 7, lettera a), della direttiva 95/46/CE). Cfr. Gruppo di lavoro Articolo 29, Parere 15/2011 sulla definizione di consenso (WP 187), per esempi sull'adeguatezza del consenso come base legittima. In tale parere, il Gruppo di lavoro ha fornito linee guida atte a distinguere il caso in cui il consenso costituisca una base lecita appropriata rispetto ai casi in cui è sufficiente fare affidamento su motivi di interesse legittimo (magari offrendo un'opportunità di rinuncia, *"opt-out"*) o sarebbe raccomandabile fondare il trattamento su un rapporto contrattuale. Cfr. anche il parere 06/2014 del Gruppo di lavoro, sezione III.1.2, pag. 17 e successive. Il consenso esplicito è anche una delle esenzioni al divieto di trattamento di categorie particolari di dati: cfr. articolo 9 del regolamento generale sulla protezione dei dati.

[10] Per orientamenti in merito alle attività di trattamento in corso basate sul consenso di cui alla direttiva 95/46, cfr. il capitolo 7 del presente documento e il considerando 171 del regolamento generale sulla protezione dei dati.

[11] In svariati pareri il Gruppo di lavoro Articolo 29 ha esaminato i limiti del consenso in situazioni in cui non sia possibile esprimerlo liberamente. Ciò è avvenuto in particolare nei seguenti documenti del Gruppo: parere 15/2011 sulla definizione di consenso (WP 187), documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (WP 131), parere 8/2001 sul trattamento dei dati personali nel contesto lavorativo (WP 48) e *"Second opinion 4/2009 on processing of data by the World Anti-Doping Agency (WADA) (International Standard for the Protection of Privacy and Personal Infor-*

mation, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations" [Secondo parere 4/2009 sul trattamento dei dati da parte dell'Agenzia mondiale antidoping (AMA) - norma internazionale per la tutela della vita privata e delle informazioni personali, sulle relative disposizioni del codice AMA e sulla altre questioni relative alla tutela della vita privata nel contesto della lotta contro il doping nello sport da parte dell'AMA e delle organizzazioni (nazionali) antidoping] (WP 162).

[12] Cfr. parere 15/2011 sulla definizione di consenso (WP 187), pag. 13.

[13] Cfr. considerando 42 e 43 del regolamento generale sulla protezione dei dati e il parere del Gruppo di lavoro 15/2011 sulla definizione di consenso, adottato il 13 luglio 2011 (WP 187), pag. 13.

[14] Il considerando 43 del regolamento generale sulla protezione dei dati afferma: *"Per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica. (...)".*

[15] Cfr. articolo 6 del regolamento generale sulla protezione dei dati, in particolare il paragrafo 1 lettera c) e lettera e).

[16] Ai fini di questo esempio, con "scuola pubblica" si intende una scuola finanziata con fondi pubblici o qualsiasi struttura educativa che si qualifica come un'autorità pubblica o un ente pubblico ai sensi della legislazione nazionale.

[17] Cfr. anche l'articolo 88 del regolamento generale sulla protezione dei dati, nel quale si sottolinea la necessità di tutelare gli interessi specifici dei dipendenti e si crea una possibilità di deroga nel diritto degli Stati membri. Cfr. anche il considerando 155.

[18] Cfr. parere 15/2011 sulla definizione di consenso (WP 187), pagg. 13-15; parere 8/2001 sul trattamento dei dati personali nel contesto lavorativo (WP 48), capitolo 10; documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro (WP 55), punto 4.2; e parere 2/2017 sul trattamento dei dati sul posto di lavoro (WP 249), punto 6.2.

[19] Cfr. parere 2/2017 sul trattamento dei dati sul posto di lavoro, pagg. 6-7.

[20] Cfr. anche il parere 2/2017 sul trattamento dei dati sul lavoro (WP 249), punto 6.2.

[21] L'articolo 7, paragrafo 4, del regolamento generale sulla protezione dei dati recita: *"Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto".* Cfr. anche il considerando 43 del regolamento, che afferma: *"[...] Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione".*

[22] Per maggiori informazioni ed esempi, cfr. parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE, adottato dal Gruppo di lavoro, il 9 aprile 2014, pagg. 19-20. (WP 217).

[23] La base legittima appropriata in tal caso potrebbe infatti essere l'articolo 6, paragrafo 1, lettera b) (contratto).

[24] Cfr. anche l'articolo 7, paragrafo 1, del regolamento generale sulla protezione dei dati, il quale stabilisce che il titolare del trattamento deve dimostrare che il consenso dell'interessato è stato liberamente manifestato.

[25] In una certa misura, l'introduzione di questo paragrafo è una codifica delle linee guida esistenti formulate dal Gruppo di lavoro. Come descritto nel parere 15/2011, quando un interessato si trova in una situazione di dipendenza rispetto al titolare del trattamento dei dati, in ragione della natura della relazione o di circostanze speciali, potrebbe sussistere una marcata presunzione che la libera manifestazione del consenso sia limitata in tali contesti (ad esempio in un rapporto di lavoro o se la raccolta dei dati è effettuata da un'autorità pubblica). Con l'entrata in vigore dell'articolo 7, paragrafo 4, sarà più difficile per il titolare del trattamento dimostrare che l'interessato ha prestato liberamente il consenso. Cfr.: parere 15/2011 sulla definizione di consenso (WP 187), pp. 14-19.

[26] Ulteriori indicazioni sulla determinazione delle "finalità" sono riportate nel documento *Opinion 3/2013 on purpose limitation* [parere 3/2013 sulla limitazione della finalità] (WP 203).

[27] Il considerando 43 del regolamento generale sulla protezione dei dati afferma che, se del caso, sarà necessario un consenso separato per trattamenti distinti. Dovrebbero essere messe a disposizione opzioni di consenso granulare in maniera da consentire agli interessati di acconsentire separatamente a finalità distinte.

[28] Cfr. parere del Gruppo di lavoro 3/2013 sulla limitazione della finalità (WP 203), pag. 16: *"Per questi motivi, una finalità che sia vaga o generica, come ad esempio 'migliorare l'esperienza degli utenti', 'finalità di marketing', 'finalità di sicurezza informatica' o 'ricerca futura', senza ulteriori dettagli, di solito non soddisfa i criteri per essere 'specifica'"*.

[29] Ciò è coerente con il parere del Gruppo di lavoro 15/2011 sulla definizione di consenso (WP 187), ad esempio a pag. 19.

[30] Cfr. anche considerando 42 del regolamento generale sulla protezione dei dati: *"[...] Ai fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali. [...]"*.

[31] Ancora una volta, cfr. considerando 42 del regolamento generale sulla protezione dei dati.

[32] Cfr. anche Gruppo di lavoro Articolo 29, Parere 15/2011 sulla definizione di consenso (WP 187), pagg. 22-23.

[33] Cfr. articolo 7, paragrafo 3, del regolamento generale sulla protezione dei dati.

[34] Cfr. anche le linee guida del Gruppo di lavoro sul processo decisionale automatizzato e la profilazione ai fini del regolamento 2016/679 (WP 251), punto IV.B, pag. 20 e successive.

[35] Ai sensi dell'articolo 49, paragrafo 1, lettera a), sono richieste informazioni specifiche sull'assenza delle garanzie di cui all'articolo 46, quando si richiede il consenso esplicito. Cfr. anche Gruppo di lavoro Articolo 29, Parere 15/2011 sulla definizione di consenso (WP 187), pag. 20.

[36] La dichiarazione di consenso deve essere designata come tale. Scrivere formulazioni del tipo "So che..." non soddisfa il requisito di un linguaggio chiaro.

[37] Cfr. articolo 4, punto 11 e articolo 7, paragrafo 2, del regolamento generale sulla protezione dei dati.

[38] Cfr. anche il considerando 58 relativo a informazioni comprensibili per i minori.

[39] Cfr. anche il considerando 42 e la direttiva 93/13/CE, in particolare l'articolo 5 (linguaggio comprensibile e, in caso di dubbio, prevale l'interpretazione più favorevole al

consumatore) e l'articolo 6 (invalidità di clausole abusive, il contratto continua a sussistere senza tali clausole abusive soltanto qualora sia ancora ragionevole, altrimenti l'intero contratto non è valido).

[40] Si noti che quando l'identità del titolare del trattamento o la finalità del trattamento non è evidente dal primo livello di informazioni dell'informativa sulla protezione dei dati a più livelli (e si trovano in ulteriori sottolivelli), sarà difficile per il titolare del trattamento dimostrare che l'interessato ha espresso il proprio consenso informato, a meno che il titolare del trattamento non possa dimostrare che l'interessato in questione ha avuto accesso a tali informazioni prima di manifestare il proprio consenso.

[41] Cfr. Documento di lavoro dei servizi della Commissione, Valutazione d'impatto, allegato 2, pag. 20 e anche pagg. 105-106 (in inglese): *"Come sottolineato anche nel parere adottato dal Gruppo di lavoro Articolo 29 in materia di consenso, sembra fondamentale chiarire che affinché un consenso sia valido è necessario ricorrere a meccanismi che non lascino dubbi circa l'intenzione dell'interessato di acconsentire, pur chiarendo che, nel contesto dell'ambiente online, l'uso di opzioni predefinite che l'interessato è tenuto a modificare per rifiutare il trattamento ('consenso basato sul silenzio') non costituisce di per sé un consenso inequivocabile. Ciò darebbe alle persone un controllo maggiore sui propri dati, qualora il trattamento si basi sul loro consenso. Per quanto riguarda l'impatto sui titolari del trattamento dei dati, ciò non avrebbe un impatto rilevante poiché chiarisce e specifica meglio le implicazioni della direttiva attuale in relazione alle condizioni per ottenere un consenso valido e significativo da parte dell'interessato. In particolare, nella misura in cui il consenso 'esplicito' chiarisca (sostituendo 'inequivocabile') le modalità e la qualità del consenso e che non è inteso a estendere i casi e le situazioni in cui il consenso (esplicito) verrebbe utilizzato come base giuridica per il trattamento, l'impatto di tale misura sui titolari del trattamento non dovrebbe essere rilevante".*

[42] Cfr. articolo 7, paragrafo 2. Cfr. Documento di lavoro 02/2013 sull'ottenimento del consenso per i cookie (WP 208), pagg. 3-6.

[43] Cfr. considerando 32 del regolamento generale sulla protezione dei dati.

[44] Il Gruppo di lavoro ha sostenuto questa posizione in maniera coerente fin dal parere 15/2011 sulla definizione di consenso (WP 187), pagg. 35-37.

[45] Ai sensi dell'articolo 49, paragrafo 1, lettera a), del regolamento generale sulla protezione dei dati, il consenso esplicito può revocare il divieto di trasferimenti di dati verso paesi che non dispongono di livelli adeguati di protezione dei dati a norma di legge. Si consulti anche il documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1 della direttiva 95/46/CE del 24 ottobre 1995 (WP 114), pag. 11, nell'ambito del quale il Gruppo di lavoro ha indicato che il consenso per i trasferimenti di dati che si verificano periodicamente o su base continuativa è inappropriato.

[46] All'articolo 22 il regolamento generale sulla protezione dei dati introduce disposizioni destinate a proteggere gli interessati da un processo decisionale basato esclusivamente sul trattamento automatizzato, nonché dalla profilazione. Le decisioni adottate su tale base sono consentite nel rispetto di determinate condizioni legali. Il consenso svolge un ruolo chiave in questo meccanismo di protezione, in quanto l'articolo 22, paragrafo 2, lettera c), del regolamento generale sulla protezione dei dati, chiarisce che un titolare del trattamento può svolgere un processo decisionale automatizzato, compresa la profilazione, che può influire in maniera significativa sulle persone fisiche, con il consenso esplicito dell'interessato. Il Gruppo di lavoro ha prodotto linee guida distinte su questo tema: Gruppo di lavoro Articolo 29, *Guidelines on Automated decision-making and Profiling for the purposes*

of Regulation 2016/679 [Linee guida sul processo decisionale automatizzato e la profilazione ai fini del regolamento 2016/679], 3 ottobre 2017 (WP 251).

[47] Cfr. anche Gruppo di lavoro Articolo 29, Parere 15/2011 sulla definizione di consenso (WP 187), pag. 29.

[48] Questo esempio non pregiudica il regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

[49] Cfr. linee guida del Gruppo di lavoro sulla trasparenza. [Citazione da finalizzare quando disponibile]

[50] Il Gruppo di lavoro ha discusso questo argomento nel parere sul consenso [cfr. parere 15/2011 sulla definizione di consenso (WP 187), pagg. 11, 14, 23, 32 e 38-39] e, tra l'altro, nel parere sull'uso dei dati relativi all'ubicazione. [cfr. parere 5/2005 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto (WP 115), pag. 7].

[51] Cfr. anche i seguenti pareri del Gruppo di lavoro: parere 4/2010 sul codice di condotta europeo della FEDMA per l'utilizzazione dei dati personali nel marketing diretto (WP 174) e parere 5/2005 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto (WP 115).

[52] Il considerando 39 del regolamento generale sulla protezione dei dati, che fa riferimento ai suoi articoli 13 e 14, afferma che *"[è] opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento"*.

[53] Cfr. articolo 17, paragrafo 1, lettera b) e articolo 17, paragrafo 3 del regolamento generale sulla protezione dei dati.

[54] In tal caso, l'altra finalità che giustifica il trattamento deve disporre di una propria base legittima distinta. Ciò non significa che il titolare del trattamento possa passare dal consenso a un'altra base legittima, cfr. la seguente sezione 6.

[55] Cfr. articolo 17, comprese le eccezioni che possono essere applicabili, e il considerando 65 del regolamento generale sulla protezione dei dati.

[56] Cfr. anche articolo 5, paragrafo 1, lettera e), del regolamento generale sulla protezione dei dati.

[57] Ai sensi dell'articolo 13, paragrafo 1, lettera c) e/o dell'articolo 14, paragrafo 1, lettera c), il titolare del trattamento è tenuto a informarne l'interessato.

[58] Fatta salva la possibilità per il diritto degli Stati membri di derogare al limite di età, cfr. articolo 8, paragrafo 1.

[59] Il considerando 58 del regolamento generale sulla protezione dei dati riafferma questo obbligo, dichiarando che, se del caso, il titolare del trattamento dovrebbe assicurarsi di fornire informazioni comprensibili per i minori.

[60] Ai sensi dell'articolo 4, paragrafo 25, del regolamento generale sulla protezione dei dati, per servizio della società dell'informazione si intende un servizio di cui all'articolo 1, paragrafo 1, lettera b), della direttiva 2015/1535: *"b) 'servizio': qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Ai fini della presente definizione si intende per: i) 'a distanza': un servizio fornito senza la presenza simultanea delle parti; ii) 'per via elettronica': un servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento (compresa la compressione digitale) e di memorizzazione di dati, e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici o altri mezzi elettromagnetici; iii) 'a richiesta individuale di un destinatario di servizi': un servizio fornito mediante trasmissione di dati su richiesta individuale"*. Nell'allegato I di detta direttiva figura un elen-

co indicativo di servizi non contemplati da tale definizione. Cfr. anche il considerando 18 della direttiva 2000/31/CE.

[61] Secondo la Convenzione delle Nazioni Unite sulla protezione dei minori, articolo 1, *"[…] si intende per fanciullo ogni essere umano avente un'età inferiore a diciott'anni, salvo se abbia raggiunto prima la maturità in virtù della legislazione applicabile"*, cfr. Nazioni Unite, risoluzione 44/25 dell'Assemblea Generale del 20 novembre 1989 (Convenzione sui diritti del fanciullo).

[62] Cfr. Corte di giustizia, 2 dicembre 2010, causa C-108/09, (Ker-Optika), punti 22 e 28. In relazione ai "servizi compositi", il Gruppo di lavoro fa riferimento anche alla causa C-434/15 *(Asociacion Profesional Elite Taxi/Uber Systems Spain SL)*, punto 40, al quale si afferma che un servizio della società dell'informazione che costituisce parte integrante di un servizio generale la cui componente principale non è un servizio della società dell'informazione (in questo caso un servizio di trasporto), non rientra nella qualificazione di "servizio della società dell'informazione".

[63] Sebbene non sia una soluzione ideale in tutti i casi, è un esempio per rispondere a tale disposizione.

[64] Cfr. Gruppo di lavoro Articolo 29, *Opinion 5/2009 on social networking services* [Parere 5/2009 sui servizi di rete sociale] (WP 163) (in inglese).

[65] Il Gruppo di lavoro osserva che non sempre il titolare della responsabilità genitoriale è il genitore naturale del minore e che la responsabilità genitoriale può essere detenuta da più parti che possono comprendere tanto persone fisiche quanto persone giuridiche.

[66] Ad esempio a un genitore o un tutore potrebbe essere chiesto di effettuare un pagamento di 0,01 EUR al titolare del trattamento tramite una transazione bancaria, nonché una breve conferma nella riga descrittiva della transazione che il titolare del conto bancario è titolare della responsabilità genitoriale rispetto all'utente. Se del caso, dovrebbe essere previsto un metodo alternativo di verifica per evitare un indebito trattamento discriminatorio nei confronti delle persone che non dispongono di un conto bancario.

[67] Inoltre, gli interessati dovrebbero essere consapevoli del diritto all'oblio di cui all'articolo 17, che è particolarmente rilevante per il consenso dato quando l'interessato era ancora un minore, cfr. considerando 63.

[68] Cfr. anche il considerando 161 del regolamento generale sulla protezione dei dati.

[69] L'articolo 6, paragrafo 1, lettera c), può anche essere applicabile a parti dei trattamenti specificamente richiesti dalle disposizioni di legge, come la raccolta di dati affidabili e solidi secondo il protocollo approvato dallo Stato membro ai sensi del regolamento sulla sperimentazione clinica.

[70] La sperimentazione specifica di medicinali può aver luogo sulla base di una legislazione UE o nazionale ai sensi dell'articolo 9, paragrafo 2, lettera i).

[71] Cfr. ad esempio il considerando 156. Il trattamento di dati personali a fini scientifici dovrebbe inoltre essere conforme ad altre normative pertinenti come quella sulle sperimentazioni cliniche; cfr. considerando 156 che menziona il regolamento (UE) n. 536/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, sulla sperimentazione clinica di medicinali per uso umano. Cfr. anche il parere del Gruppo di lavoro 15/2011 sulla definizione di consenso (WP 187), pag. 8: *"l'ottenimento del consenso non esonera il titolare del trattamento dagli obblighi di cui all'articolo 6 con riferimento ai principi di lealtà, necessità e proporzionalità, oltre che di qualità dei dati. Per esempio, anche qualora il trattamento dei dati personali poggi sul consenso dell'utilizzatore, ciò di per sé non legittima una raccolta dei dati supplementare rispetto allo scopo specifico. […] In linea di principio, il consenso non dev'essere consi-*

derato come una forma di esonero dagli altri principi di protezione dei dati, bensì come una salvaguardia. Esso è, in prima linea, un motivo di liceità e non comporta una rinuncia all'applicazione di altri principi".

[72] Possono essere pertinenti anche altre misure di trasparenza. Quando i titolari del trattamento svolgono un trattamento di dati a fini scientifici, nonostante non sia possibile fornire informazioni complete sin dall'inizio, possono comunque designare un referente specifico al quale gli interessati possono rivolgere eventuali quesiti.

[73] Tale possibilità si può riscontrare nell'articolo 14, paragrafo 1, dell'attuale legge sui dati personali della Finlandia (*Henkilötietolaki*, 523/1999).

[74] Cfr. anche il parere del Gruppo di lavoro 05/2014 sulle tecniche di anonimizzazione (WP 216).

[75] Nei casi in cui determinate attività di trattamento dei dati sono limitate ai sensi dell'articolo 18, può essere necessario il consenso dell'interessato per annullare le limitazioni interessate.

[76] Il considerando 171 del regolamento generale sulla protezione dei dati afferma: *"Il presente regolamento dovrebbe abrogare la direttiva 95/46/CE. Il trattamento già in corso alla data di applicazione del presente regolamento dovrebbe essere reso conforme al presente regolamento entro un periodo di due anni dall'entrata in vigore del presente regolamento. Qualora il trattamento si basi sul consenso a norma della direttiva 95/46/CE, non occorre che l'interessato presti nuovamente il suo consenso, se questo è stato espresso secondo modalità conformi alle condizioni del presente regolamento, affinché il titolare del trattamento possa proseguire il trattamento in questione dopo la data di applicazione del presente regolamento. Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate".*

[77] Come indicato nell'introduzione, il regolamento generale sulla protezione dei dati fornisce ulteriori chiarimenti e specifiche sui requisiti per ottenere e dimostrare un consenso valido. Molti dei nuovi requisiti si basano sul parere 15/2011 sul consenso.

Linee guida sulla trasparenza ai sensi del regolamento 2016/679 [WP 260 rev. 01]

Adottate il 29 novembre 2017
Versione emendata adottata l'11 aprile 2018

IL GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 della stessa,

visto il suo regolamento interno,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della direzione generale Giustizia, Commissione europea, B - 1049 Bruxelles, Belgio, ufficio MO-59 02/013.

Sito Internet: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Indice

TOC (*)

INTRODUZIONE

1. Le presenti linee guida riportano gli orientamenti pratici e l'assistenza interpretativa offerta dal Gruppo di lavoro articolo 29 ("Gruppo") sul nuovo obbligo di trasparenza relativo al trattamento dei dati personali ai sensi del regolamento generale sulla protezione dei dati ("regolamento")[1]. La trasparenza è un obbligo trasversale a norma del regolamento, che si esplica in tre elementi centrali: 1) la fornitura agli interessati d'informazioni relative al trattamento corretto; 2) le modalità con le quali il titolare del trattamento comunica con gli interessati riguardo ai diritti di cui godono ai sensi del regolamento; 3) le modalità con le quali il titolare del trattamento agevola agli interessati l'esercizio dei diritti di cui godono[2]. Nella misura in cui il rispetto della trasparenza è imposto con riferimento al trattamento dei dati ai sensi della direttiva (UE) 2016/680[3], le presenti linee guida si applicano anche all'interpretazione di tale principio[4]. Come tutte quelle emanate dal Gruppo, anche le presenti linee guida sono da intendersi come applicabili in generale ai titolari del trattamento, a prescindere dalle specifiche a livello settoriale o normativo tipiche per l'uno o l'altro di essi. Non possono quindi cogliere tutte le sfumature e le numerose variabili che possono presentarsi nel contesto degli obblighi di trasparenza di uno specifico settore o di un'area regolamentata. Mirano tuttavia a consentire ai titolari del trattamento di comprendere, a un livello elevato, come il Gruppo interpreti gli effetti pratici degli obblighi di trasparenza e a indicare l'approccio che, secondo il Gruppo, i titolari del trattamento dovrebbero adottare per essere trasparenti, ricomprendendo al contempo correttezza e responsabilizzazione nelle loro misure di trasparenza.

2. La trasparenza è un aspetto che da tempo si è consolidato nel diritto dell'Unione europea[5]. Mira a infondere fiducia nei processi che riguardano i cittadini, permettendo loro di comprenderli e, se necessario, di opporvisi. Inoltre, è espressione del principio di correttezza in relazione al trattamento dei dati personali affermato all'articolo 8 della Carta dei diritti fondamentali dell'Unione europea. Ai sensi dell'articolo 5, paragrafo 1, lettera a), del regolamento[6], oltre ai requisiti che il trattamento dei dati sia lecito e corretto, la trasparenza è ora inclusa in quanto elemento fondamentale di questi principi[7]. La trasparenza è intrinsecamente legata alla correttezza e al nuovo principio di responsabilizzazione ai sensi del

(*) *NDR. L'indice non è stato inserito, per errore, nella versione ufficiale delle linee guida. Il documento è qui riproposto come nel documento originale.*

regolamento. Dall'articolo 5, paragrafo 2, risulta inoltre che il titolare del trattamento dev'essere sempre in grado di dimostrare che i dati personali sono trattati in modo trasparente nei confronti dell'interessato[8]. A questo si aggiunge il fatto che il principio di responsabilizzazione impone la trasparenza delle operazioni di trattamento affinché il titolare del trattamento sia in grado di dimostrare il rispetto degli obblighi che il regolamento gli impone[9].

3. Secondo il considerando 171 del regolamento, laddove il trattamento sia già in corso prima del 25 maggio 2018, il titolare del trattamento dovrebbe garantirne la conformità agli obblighi di trasparenza alla data del 25 maggio 2018 (così come a tutti gli altri obblighi previsti dal regolamento). Ciò significa che prima del 25 maggio 2018 il titolare del trattamento dovrebbe revisionare tutte le informazioni fornite agli interessati riguardo al trattamento dei dati personali che li riguardano (ad esempio in dichiarazioni/informative sulla privacy, ecc.), al fine di garantire l'adempimento degli obblighi di trasparenza esaminati nelle presenti linee guida. In caso di modifiche o aggiunte a tali informazioni, il titolare del trattamento dovrebbe esplicitare agli interessati che esse discendono dall'esigenza di conformarsi al regolamento. Il Gruppo raccomanda di portare tali modifiche o aggiunte attivamente all'attenzione degli interessati, ma il titolare del trattamento dovrebbe perlomeno mettere le informazioni a disposizione del pubblico (ad es. sul suo sito web). Se sono di carattere materiale o sostanziale, in linea con i paragrafi 29-32 *infra* le modifiche o le aggiunte dovrebbero tuttavia essere portate attivamente all'attenzione dell'interessato.

4. Quando il titolare del trattamento la rispetta, la trasparenza consente agli interessati di imputare la responsabilità al titolare e al responsabile del trattamento e di esercitare il controllo sui dati personali che li riguardano, ad esempio dando o revocando il consenso informato e attivando i loro diritti di interessati[10]. Nel regolamento il concetto di trasparenza non è legalistico, ma piuttosto incentrato sull'utente e si concreta in vari articoli contenenti gli specifici obblighi imposti ai titolari e ai responsabili del trattamento. Gli obblighi concreti (d'informazione) sono indicati negli articoli 12-14 del regolamento. A ogni modo, la qualità, l'accessibilità e la comprensibilità delle informazioni sono altrettanto importanti del contenuto effettivo delle informazioni finalizzate alla trasparenza che devono essere fornite agli interessati.

5. Gli obblighi di trasparenza imposti dal regolamento si applicano a prescindere dalla base giuridica del trattamento e per tutto il ciclo di vita dello stesso. Ciò risulta chiaro dall'articolo 12, il quale stabilisce che la trasparenza si applica nelle seguenti fasi del ciclo di trattamento dei dati:

   - prima o all'inizio del ciclo di trattamento dei dati, vale a dire quando i dati personali sono raccolti presso l'interessato od ottenuti in altro modo;

- nell'arco dell'intero ciclo di vita del trattamento, ovvero nella comunicazione con gli interessati sui loro diritti;
- in momenti specifici in cui il trattamento è in corso, ad esempio quando si verifica una violazione di dati oppure in caso di modifica rilevante del trattamento.

IL SIGNIFICATO DELLA TRASPARENZA

6. Il concetto di trasparenza non è definito nel regolamento. Il considerando 39 del regolamento ne illustra il significato e l'effetto nell'ambito del trattamento dei dati:

   "Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano...".

ELEMENTI DELLA TRASPARENZA AI SENSI DEL REGOLAMENTO

7. Applicandosi ai diritti dell'interessato, gli articoli fondamentali per quanto concerne la trasparenza nel regolamento si trovano nel capo III (Diritti dell'interessato). L'articolo 12 fissa le regole generali che si applicano alla fornitura d'informazioni agli interessati (ai sensi degli articoli 13 e 14), alla comunicazione con gli interessati riguardo all'esercizio dei loro diritti (ai sensi degli articoli 15-22) e alle comunicazioni relative alle violazioni di dati (articolo 34). In particolare, l'articolo 12 impone che le informazioni o le comunicazioni in questione debbano rispettare i criteri seguenti:

   - devono essere concise, trasparenti, intelligibili e facilmente accessibili (articolo 12, paragrafo 1);
   - devono essere formulate con un linguaggio semplice e chiaro (articolo 12, paragrafo 1);
   - il requisito di un linguaggio semplice e chiaro è di particolare importanza nel caso d'informazioni destinate ai minori (articolo 12, paragrafo 1);
   - devono essere fornite per iscritto "o con altri mezzi, anche, se del caso, con mezzi elettronici" (articolo 12, paragrafo 1);
   - se richiesto dall'interessato, possono essere fornite oralmente (articolo 12, paragrafo 1);
   - devono essere in genere gratuite (articolo 12, paragrafo 5).

"Concise, trasparenti, intelligibili e facilmente accessibili"

8. L'obbligo di fornire agli interessati le informazioni e le comunicazioni in forma "concisa e trasparente" implica che il titolare del trattamento presenti le informazioni/comunicazioni in maniera efficace e succinta al fine di evitare un subissamento informativo. Tali informazioni dovrebbero essere differenziate nettamente da altre che non riguardano la vita privata, quali clausole contrattuali o condizioni generali d'uso. Nell'ambiente online l'utilizzo di una dichiarazione/informativa sulla privacy stratificata consentirà all'interessato di consultarne immediatamente la specifica sezione desiderata, senza dover scorrere ampie porzioni di testo alla ricerca di un argomento in particolare.

9. L'obbligo di fornire informazioni "intelligibili" implica che risultino comprensibili a un esponente medio del pubblico cui sono dirette. L'intelligibilità è strettamente connessa all'obbligo di utilizzare un linguaggio semplice e chiaro. Il titolare dei dati responsabilizzato saprà su che tipo di persone raccoglie informazioni e potrà utilizzare tali conoscenze per stabilire che cosa è probabile che il pubblico in questione comprenda. Ad esempio, il titolare che raccoglie dati personali di professionisti potrà immaginare che il suo pubblico presenti un livello di comprensione superiore rispetto a quello cui si rivolge il titolare che ottiene dati personali di minori. Se non è certo del livello di intelligibilità e trasparenza delle informazioni e dell'efficacia delle interfacce utente/informative/dichiarazioni, ecc., il titolare può effettuare dei test, ad esempio ricorrendo, secondo il caso, a meccanismi quali gruppi di utenti, test di leggibilità, interazioni formali e informali e dialoghi con gruppi di settore, associazioni dei consumatori ed enti normativi.

10. Una considerazione centrale al principio della trasparenza evidenziata in queste disposizioni è che l'interessato dovrebbe essere in grado di determinare in anticipo quali siano la portata del trattamento e le relative conseguenze e non dovrebbe successivamente essere colto di sorpresa dalle modalità di utilizzo dei dati personali che lo riguardano. Ciò costituisce un aspetto importante del principio di correttezza di cui all'articolo 5, paragrafo 1, del regolamento ed è altresì connesso al considerando 39, il quale stabilisce che *"[è] opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali..."*. In particolare per il trattamento di dati in casi complessi, tecnici o inattesi, la posizione del Gruppo è che, oltre a fornire le informazioni prescritte agli articoli 13 e 14 (di cui ci si occuperà nel prosieguo delle presenti linee guida), il titolare del trattamento debba dichiarare in una sede distinta, in un linguaggio privo di ambiguità, quali saranno le principali conseguenze del trattamento, in altre parole, quale tipo di effetto sull'interessato, descritto in una dichiarazione/informativa sulla privacy, avrà concretamente il trattamento specifico. Conformemente al principio di responsabilizzazione e in linea con il considerando 39, il titolare del trattamento dovrebbe valutare se questo tipo di trattamento presenti per le persone fisiche rischi particolari da segnalare loro. Ciò può contribui-

re a offrire una panoramica dei tipi di trattamento che potrebbero avere l'impatto più forte sui diritti e libertà fondamentali degli interessati in relazione alla protezione dei dati personali che li riguardano.

11. L'elemento della "facile accessibilità" implica che l'interessato non sia costretto a cercare le informazioni, ma che anzi gli sia immediatamente chiaro dove e come queste siano accessibili, ad esempio perché gli sono fornite direttamente, un link lo dirige verso di esse o le informazioni sono contrassegnate chiaramente oppure perché le informazioni si configurano come risposta a una domanda in linguaggio naturale (ad esempio in una dichiarazione/informativa sulla privacy stratificata online, in FAQ, mediante pop-up contestuali che si attivano quando l'interessato compila un modulo online oppure, in un contesto digitale interattivo, attraverso un'interfaccia chatbot, ecc. Questi meccanismi sono trattati nel dettaglio in seguito, tra cui ai paragrafi 33-40.

Esempio

Tutte le organizzazioni che hanno un sito Internet dovrebbero pubblicarvi una dichiarazione/informativa sulla privacy. Su ogni pagina del sito dovrebbe essere chiaramente visibile un link diretto alla dichiarazione/informativa sulla privacy che riporti una dicitura di uso comune (come "Privacy", "Informativa sulla privacy" o "Informativa sulla protezione dei dati"). Non sono considerati facilmente accessibili un posizionamento o codici cromatici tali da rendere il testo o il link meno visibile o difficile da individuare in una pagina Internet.

Per le app le informazioni necessarie dovrebbero essere messe a disposizione presso uno store online prima del download. Una volta installata l'app, le informazioni devono continuare a essere facilmente accessibili al suo interno. Un modo per soddisfare questo requisito consiste nel garantire che le informazioni non siano mai a più di due "tocchi" di distanza (ad es. includendo un'opzione "Privacy"/"Protezione dei dati" nella funzione di menù dell'app). Inoltre, l'informativa sulla privacy dovrebbe essere specifica alla app e non meramente l'informativa generica dell'azienda che è proprietaria dell'app o che la mette a disposizione pubblicamente.

Il Gruppo raccomanda come migliore prassi che, al momento della raccolta dei dati personali in ambiente online, sia fornito un link alla dichiarazione/informativa sulla privacy o che tali informazioni siano messe a disposizione sulla stessa pagina in cui sono raccolti i dati personali.

"Linguaggio semplice e chiaro"

12. Se le informazioni sono scritte (e, nel caso in cui le informazioni scritte siano fornite oralmente, o con metodi audio/audiovisivi, fra l'altro per interessati con disabilità visive), si devono seguire le migliori prassi per una

scrittura chiara[11]. Un analogo requisito linguistico (di un "linguaggio chiaro e comprensibile") è stato precedentemente utilizzato dal legislatore dell'Unione europea[12]; ad esso è fatto esplicito riferimento nel considerando 42 del regolamento[13] in relazione al consenso. Il fatto che il linguaggio debba essere semplice e chiaro significa che le informazioni dovrebbero essere fornite nel modo più semplice possibile, evitando frasi e strutture linguistiche complesse. Le informazioni dovrebbero essere concrete e certe, non dovrebbero essere formulate in termini astratti o ambigui né lasciare spazio a interpretazioni multiple. In particolare dovrebbero risultare chiare le finalità e la base giuridica del trattamento dei dati personali.

Esempi di cattive prassi

Le espressioni seguenti non sono sufficientemente chiare con riferimento alle finalità del trattamento:

- *"I tuoi dati personali potrebbero essere usati per sviluppare nuovi servizi"* (non essendo chiaro quali siano i "servizi" o come i dati contribuiranno al loro sviluppo);
- *"I tuoi dati personali potrebbero essere usati per finalità di ricerca"* (non essendo chiaro a quale tipo di "ricerca" si faccia riferimento);
- *"I tuoi dati personali potrebbero essere usati per offrire servizi personalizzati"* (non essendo chiaro che cosa implichi la "personalizzazione").

Esempi di buone prassi[14]

- *"Conserveremo lo storico dei tuoi acquisti e utilizzeremo i dati sui prodotti da te precedentemente acquistati per suggerirti altri prodotti che riteniamo siano di tuo interesse"* (è chiaro quali tipi di dati saranno trattati, che l'interessato riceverà pubblicità mirata di prodotti e che i suoi dati personali saranno utilizzati a tal fine).
- *"Conserveremo e valuteremo informazioni sulle tue recenti visite del nostro sito Internet e sul modo in cui navighi nelle sue diverse sezioni per finalità di analisi volte a comprendere come è usato il nostro sito, così da renderlo più intuitivo"* (è chiaro quali tipi di dati saranno trattati e il tipo di analisi che effettuerà il titolare del trattamento).
- *"Registreremo gli articoli del nostro sito da te consultati e useremo le informazioni così ottenute per inviarti, su questo sito Internet, pubblicità mirata che risponda ai tuoi interessi, da noi individuati sulla base degli articoli che hai letto"* (è chiaro che cosa implica la personalizzazione e quali interessi attribuiti all'interessato sono stati individuati).

13. Si dovrebbe evitare l'uso di qualificatori linguistici come "può", "potrebbe", "alcuni", "spesso" e "possibile". Se il titolare del trattamento sceglie di usa-

re un linguaggio vago, conformemente al principio di responsabilizzazione dovrebbe essere in grado di dimostrare il motivo per cui tale linguaggio è inevitabile e il motivo per cui non compromette la correttezza del trattamento. Paragrafi e frasi dovrebbero essere ben strutturati, utilizzando pallini e rientri per segnalare rapporti gerarchici. Si dovrebbe prediligere la forma attiva a quella passiva ed evitare l'uso eccessivo di costruzioni nominali. Le informazioni fornite all'interessato non dovrebbero contenere linguaggio o terminologia eccessivamente legalistica, tecnica o specialistica. Se le informazioni sono tradotte in una o più lingue, il titolare del trattamento dovrebbe accertare che tutte le traduzioni siano corrette e che, nella o nelle altre lingue, la fraseologia e la sintassi risultino comprensibili, in maniera tale da non costringere il lettore a decifrare o reinterpretare il testo tradotto (si dovrebbe fornire una traduzione in una o più lingue nel caso in cui il titolare del trattamento si rivolga[15] a interessati che parlano tali lingue).

Informazioni fornite a minori e ad altre persone vulnerabili

14. Il titolare del trattamento che si rivolge a minori[16] o è (o dovrebbe essere) consapevole del fatto che i suoi beni/servizi sono utilizzati soprattutto da minori (anche quando presuppone il consenso del minore[17]) dovrebbe accertare che il lessico, il tono e lo stile utilizzati siano adeguati ai minori e per loro comprensibili, così che il minore destinatario delle informazioni si renda conto che il messaggio o l'informazione sono diretti a lui[18]. Un esempio calzante di linguaggio adatto ai minori utilizzato come alternativa al linguaggio giuridico originario è la pubblicazione "I diritti dei bambini in parole semplici", che spiega in linguaggio adatto ai bambini la convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza[19].

15. La posizione assunta dal Gruppo è che la trasparenza è un diritto a se stante, che si applica tanto ai minori quanto agli adulti. Il Gruppo sottolinea in particolare che i minori non perdono i loro diritti alla trasparenza in quanto interessati semplicemente per il fatto che il consenso è stato dato/autorizzato dal titolare della responsabilità genitoriale in una situazione in cui trova applicazione l'articolo 8 del regolamento. Sebbene in molti casi tale consenso sia concesso o autorizzato una tantum dal titolare della responsabilità genitoriale, il minore (come qualsiasi altro interessato) gode di un diritto permanente alla trasparenza per tutta la durata del rapporto con il titolare del trattamento. Ciò è coerente con l'articolo 13 della convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza, secondo cui il minore ha diritto alla libertà di espressione, che comprende la libertà di ricercare, di ricevere e di divulgare informazioni e idee di ogni specie[20]. È importante sottolineare che, nel disporre la prestazione del consenso per conto del minore che non ha ancora raggiunto una determinata età[21], l'articolo 8 *non prevede* misure di trasparenza dirette al titolare della responsabilità genitoriale che dà tale consenso. Pertanto, stando agli specifici rimandi alle misure di trasparenza destinate ai minori di cui all'articolo 12, paragrafo 1 (supportato dai considerando 38 e 58), il titolare del trattamento che si rivolge

a minori o che sa che i suoi beni o servizi sono utilizzati soprattutto da minori in età da essere in grado di leggere e scrivere è tenuto a garantire che le informazioni e comunicazioni siano trasmesse in un linguaggio semplice e chiaro o con un mezzo che i minori possano comprendere con facilità. Onde fugare ogni dubbio, tuttavia, il Gruppo riconosce che, nel caso di bambini molto piccoli o che non sanno ancora leggere e scrivere, le misure di trasparenza possono essere rivolte ai titolari della responsabilità genitoriale, dal momento che, nella maggior parte dei casi, tali bambini non saranno probabilmente in grado di comprendere nemmeno i messaggi più semplici relativi alla trasparenza, siano essi redatti per iscritto o comunicati diversamente.

16. Se è consapevole che i suoi beni/servizi sono utilizzati da (o destinati ad) altri soggetti vulnerabili della società, tra cui persone con disabilità o persone che possono incontrare difficoltà ad accedere alle informazioni, il titolare del trattamento dovrebbe tenere conto delle vulnerabilità di tali interessati nella valutazione del modo in cui assolvere gli obblighi di trasparenza nei loro confronti[22]. Ciò si ricollega alla necessità che il titolare del trattamento valuti il probabile livello di comprensione del proprio pubblico, come illustrato sopra al paragrafo 9.

"Per iscritto o con altri mezzi"

17. Ai sensi dell'articolo 12, paragrafo 1, la fornitura d'informazioni o comunicazioni agli interessati avviene di regola in forma scritta[23] (l'articolo 12, paragrafo 7, prevede inoltre che le informazioni siano fornite in combinazione con icone standardizzate; quest'aspetto è esaminato nella sezione sugli strumenti di visualizzazione ai paragrafi 49—53). Tuttavia, il regolamento consente anche l'utilizzo di altri mezzi non specificati, tra cui quelli elettronici. La posizione del Gruppo con riferimento ai mezzi elettronici scritti è la seguente: laddove il titolare del trattamento abbia un sito Internet (o operi, in tutto o in parte, tramite un sito Internet), è raccomandato l'uso di dichiarazioni/informative sulla privacy stratificate, che consentano ai visitatori del sito di consultare le sezioni particolari della dichiarazione/informativa sulla privacy di loro interesse (si vedano maggiori informazioni sulle dichiarazioni/informative sulla privacy stratificate ai paragrafi 35-37)[24]. Tutte le informazioni rivolte agli interessati dovrebbero comunque essere disponibili in un unico luogo o in un documento completo (in formato digitale o cartaceo), al quale essi possano accedere facilmente qualora intendano consultare nella loro interezza le informazioni di cui sono destinatari. Va rilevato che l'utilizzo dell'approccio stratificato per fornire informazioni agli interessati non è circoscritto ai mezzi elettronici scritti. Come esposto ai paragrafi 35, 36 e 38, può essere usato anche impiegando una combinazione di metodi al fine di garantire trasparenza in relazione al trattamento dei dati.

18. Ovviamente, l'utilizzo di dichiarazioni/informative sulla privacy digitali stratificate non è l'unico mezzo elettronico scritto cui i titolari del tratta-

mento possono ricorrere. Altri mezzi elettronici includono pop-up contestuali "just-in-time", notifiche touch 3D o hover-over e apposite dashboard. Gli strumenti elettronici non scritti che possono essere utilizzati *in aggiunta* alla dichiarazione/informativa sulla privacy stratificata potrebbero includere video e notifiche vocali su smartphone o IoT[25]. Gli "altri mezzi" non necessariamente elettronici potrebbero comprendere, ad esempio, vignette, infografica o diagrammi. Se le informazioni finalizzate alla trasparenza sono dirette specificamente ai minori, il titolare del trattamento dovrebbe valutare quali tipi di misure possano essere accessibili in modo particolare ai minori (tra gli altri, ad es., fumetti/vignette, pittogrammi, animazioni, ecc.).

19. Un aspetto di fondamentale importanza è che il o i metodi scelti per fornire le informazioni siano adeguati alle circostanze, vale a dire la modalità di interazione tra il titolare del trattamento e l'interessato o la modalità di raccolta delle informazioni dell'interessato. Ad esempio, limitarsi a fornire le informazioni in formato elettronico scritto, come con una dichiarazione/informativa sulla privacy online, potrebbe non essere adeguato/non funzionare nel caso in cui il dispositivo che cattura i dati personali non ha uno schermo (ad es. dispositivi IoT/smart) per accedere al sito Internet/visualizzare le informazioni scritte. In tali casi dovrebbe essere preso in considerazione un *ulteriore* mezzo alternativo adeguato, ad esempio l'inserimento della dichiarazione/informativa sulla privacy in manuali di istruzioni cartacei oppure l'indicazione, nelle istruzioni in formato cartaceo o sulla confezione, dell'indirizzo URL del sito Internet (ovvero la pagina specifica del sito) al quale è reperibile la dichiarazione/informativa sulla privacy. Se il dispositivo privo di schermo dispone di funzioni audio, si potrebbe provvedere anche la fornitura audio (orale) delle informazioni. Il Gruppo ha già formulato raccomandazioni sulla trasparenza e sulla fornitura d'informazioni agli interessati nel parere sui recenti sviluppi nel campo dell'Internet degli oggetti[26] (come l'utilizzo di codici QR stampati su tali oggetti, in maniera tale che, una volta scansionati, il codice QR visualizzi le necessarie informazioni finalizzate alla trasparenza). Tali raccomandazioni rimangono applicabili ai sensi del regolamento.

"...le informazioni possono essere fornite oralmente"

20. L'articolo 12, paragrafo 1, prevede specificamente che le informazioni possano essere fornite oralmente su richiesta dell'interessato, purché sia comprovata con altri mezzi l'identità di questi. In altre parole, il mezzo impiegato dovrebbe andare oltre il semplice fatto di basarsi sull'affermazione con cui l'interessato sostiene di essere una determinata persona e dovrebbe consentire al titolare del trattamento di identificare l'interessato con sufficiente certezza. L'obbligo di verificare l'identità dell'interessato prima di fornire informazioni oralmente si applica soltanto alle informazioni relative all'esercizio dei diritti di cui agli articoli 15-22 e all'articolo 34 da parte di uno specifico interessato. Questo prerequisito della comunicazione d'informazioni orali non può applicarsi alla fornitura delle infor-

mazioni generali sulla privacy, prevista agli articoli 13 e 14, dal momento che le informazioni richieste da detti articoli devono essere accessibili anche ai *futuri* utenti/clienti (la cui identità il titolare del trattamento non sarebbe in grado di verificare). Pertanto, le informazioni necessarie ai sensi degli articoli 13 e 14 possono essere fornite oralmente senza che il titolare del trattamento richieda la prova dell'identità dell'interessato.

21. La fornitura orale delle informazioni richieste dagli articoli 13 e 14 non implica necessariamente che le informazioni orali siano fornite individualmente (vale a dire di persona o al telefono). Possono essere fornite informazioni orali automatizzate in aggiunta a mezzi scritti. Può essere il caso, ad esempio, per le persone con disabilità visive nell'interazione con fornitori di servizi della società dell'informazione o nel contesto dei dispositivi smart senza schermo richiamati al paragrafo 19. Se il titolare del trattamento ha scelto di fornire informazioni all'interessato oralmente o se questi richiede la fornitura d'informazioni o comunicazioni orali, il Gruppo reputa che il titolare del trattamento debba consentire all'interessato di riascoltare messaggi preregistrati. È obbligatorio procedere in tal senso qualora la richiesta d'informazioni orali si riferisca a interessati con disabilità visive o ad interessati che possano incontrare difficoltà nell'accesso o nella comprensione delle informazioni scritte. Il titolare del trattamento dovrebbe altresì provvedere a conservare traccia e a poter dimostrare (ai fini della rispondenza al requisito di responsabilizzazione): i) la richiesta di fornire informazioni oralmente, ii) il metodo con cui è stata verificata l'identità dell'interessato (ove applicabile – si veda il paragrafo 20) e iii) il fatto che le informazioni sono state fornite all'interessato.

"Gratuitamente"

22. Ai sensi dell'articolo 12, paragrafo 5[27], il titolare del trattamento non può in genere addebitare alcunché all'interessato per la fornitura d'informazioni ai sensi degli articoli 13 e 14 o per le comunicazioni e azioni intraprese ai sensi degli articoli 15-22 (sui diritti degli interessati) e dell'articolo 34 (comunicazione di violazioni dei dati personali all'interessato)[28]. Quest'aspetto della trasparenza implica anche che le informazioni fornite in ossequio agli obblighi di trasparenza non possono essere subordinate ad operazioni finanziarie, ad esempio il pagamento o l'acquisto di servizi o beni[29].

INFORMAZIONI DA FORNIRE ALL'INTERESSATO – ARTICOLI 13 E 14

Contenuto

23. Il regolamento elenca le categorie d'informazioni che devono essere fornite all'interessato relativamente al trattamento dei dati personali che lo riguardano, quando i dati personali sono raccolti presso l'interessato (articolo 13) od ottenuti da altra fonte (articolo 14). La **tabella allegata** alle

presenti linee guida sintetizza le categorie d'informazioni da fornire ai sensi degli articoli 13 e 14, tenendo altresì conto della natura, della portata e del contenuto degli obblighi in questione. Per chiarezza, il Gruppo reputa che non vi sia differenza tra lo stato delle informazioni che devono essere fornite ai sensi dei paragrafi 1 e 2 dell'articolo 13 o, rispettivamente, dell'articolo 14. Tutte le informazioni previste in detti paragrafi sono di uguale importanza e devono essere fornite all'interessato.

"Misure appropriate"

24. Oltre al contenuto, sono importanti anche la forma e il modo in cui dovrebbero essere fornite le informazioni richieste dagli articoli 13 e 14. Spesso il documento contenente dette informazioni è chiamato informativa sulla protezione dei dati, informativa sulla privacy, privacy policy, dichiarazione sulla privacy o informativa sul trattamento dei dati personali. Il regolamento non contiene prescrizioni circa il formato o la modalità con cui tali informazioni dovrebbero essere fornite all'interessato, ma precisa che spetta al titolare del trattamento adottare "misure appropriate" per fornire le informazioni necessarie a fini di trasparenza. Ciò significa che il titolare del trattamento dovrebbe prendere una decisione sulla modalità e sulla forma appropriate per fornire le informazioni tenendo conto di tutte le circostanze della raccolta e del trattamento dei dati. In particolare, le misure appropriate dovranno essere valutate alla luce dell'esperienza dell'utente con il prodotto/servizio, vale a dire tenendo conto del dispositivo utilizzato (se applicabile), della natura delle interfacce utente/interazioni con il titolare del trattamento (il cosiddetto "percorso utente") e delle limitazioni che tali fattori implicano. Come osservato al paragrafo 17, il Gruppo raccomanda che, se il titolare del trattamento ha una presenza online, sia predisposta una dichiarazione/informativa sulla privacy stratificata online.

25. Come ausilio per individuare la modalità più appropriata per fornire le informazioni, sarebbe utile che, prima dell'attivazione, il titolare del trattamento sperimentasse diversi metodi mediante test sugli utenti (ad es. test di Hall o altri test standardizzati della leggibilità o accessibilità) per sondare gli utenti sull'accessibilità, comprensibilità e facilità d'uso della misura (si vedano anche gli ulteriori commenti sopra riportati, al paragrafo 9, su altri meccanismi per condurre test sugli utenti). Documentare questo approccio dovrebbe peraltro aiutare il titolare del trattamento negli obblighi di responsabilizzazione, dimostrando come lo strumento/l'approccio scelto per trasmettere le informazioni sia quello più appropriato nel caso specifico.

Tempistiche per la fornitura delle informazioni

26. Gli articoli 13 e 14 stabiliscono quali informazioni devono essere fornite all'interessato nella fase iniziale del ciclo del trattamento[30]. L'articolo 13 si applica al caso in cui i dati sono raccolti presso l'interessato. Sono compresi i dati personali che:

- l'interessato fornisce consapevolmente al titolare del trattamento (ad es. quando compila un modulo online) oppure
- il titolare del trattamento raccoglie presso l'interessato mediante osservazione (ad es. utilizzando dispositivi o software per catturare dati in modo automatizzato quali telecamere, apparecchiature di rete, tracciamento Wi-Fi, sensori RFID o di altro tipo).

L'articolo 14 trova applicazione qualora i dati personali non siano stati ottenuti presso l'interessato. Sono compresi i dati personali che il titolare del trattamento ha ottenuto da altre fonti quali:

- titolari del trattamento terzi;
- fonti pubblicamente disponibili;
- intermediari di dati;
- altri interessati.

27. Per quanto riguarda la tempistica della fornitura di queste informazioni, la tempestività è un elemento di fondamentale importanza dell'obbligo di trasparenza e dell'obbligo di trattare i dati in maniera corretta. Qualora trovi applicazione l'articolo 13, ai sensi del suo paragrafo 1 le informazioni devono essere fornite *"nel momento in cui i dati personali sono ottenuti"*. Nel caso di dati personali ottenuti indirettamente ai sensi dell'articolo 14, le tempistiche entro cui le informazioni devono essere fornite all'interessato sono stabilite al medesimo articolo, paragrafo 3, lettere da a) a c), come segue:

    - il requisito generale è che le informazioni siano fornite entro "un termine ragionevole" dall'ottenimento dei dati personali e non più tardi di un mese, *"in considerazione delle specifiche circostanze in cui i dati personali sono trattati"* (articolo 14, paragrafo 3, lettera a));

    - il limite generale di un mese di cui all'articolo 14, paragrafo 3, lettera a), può essere ulteriormente accorciato ai sensi dell'articolo 14, paragrafo 3, lettera b)[31], il quale prevede la situazione in cui i dati sono destinati alla comunicazione con l'interessato. In tal caso, le informazioni devono essere fornite al più tardi al momento della prima comunicazione con l'interessato. Se la prima comunicazione si verifica prima del limite di un mese dall'ottenimento dei dati personali, le informazioni devono essere fornite al più tardi al momento della prima comunicazione con l'interessato, nonostante non sia trascorso un mese dal momento dell'ottenimento dei dati. Se la prima comunicazione con l'interessato si verifica più di un mese dopo l'ottenimento dei dati personali, l'articolo 14, paragrafo 3, lettera a), continua a trovare applicazione; le informazioni di cui all'articolo 14 devono quindi essere fornite all'interessato al più tardi entro un mese dal loro ottenimento;

    - il limite generale di un mese di cui all'articolo 14, paragrafo 3, lettera a), può anche essere accorciato ai sensi dell'articolo 14, paragrafo 3,

lettera c)[32], il quale prevede la situazione in cui i dati sono comunicati a un altro destinatario (che si tratti o meno di un terzo)[33]. In tal caso, le informazioni devono essere fornite al più tardi al momento della prima comunicazione. Se la comunicazione si verifica prima del limite di un mese, le informazioni devono essere fornite al più tardi al momento della prima comunicazione, nonostante non sia trascorso un mese dal momento dell'ottenimento dei dati. Analogamente alla situazione dell'articolo 14, paragrafo 3, lettera b), se la comunicazione dei dati personali si verifica più di un mese dopo il loro ottenimento, l'articolo 14, paragrafo 3, lettera a), continua a trovare applicazione; le informazioni di cui all'articolo 14 devono quindi essere fornite all'interessato al più tardi entro un mese dal loro ottenimento.

28. Il limite massimo di tempo entro il quale le informazioni di cui all'articolo 14 devono essere fornite all'interessato è in ogni caso di un mese. Tuttavia, i principi di correttezza e responsabilizzazione di cui al regolamento impongono al titolare del trattamento di decidere il momento in cui fornire le informazioni di cui all'articolo 14 considerando sempre le ragionevoli aspettative degli interessati e l'effetto che il trattamento potrebbe avere sugli stessi e sulla loro capacità di esercitare i diritti di cui godono in relazione al trattamento. Il principio della responsabilizzazione impone al titolare del trattamento di dimostrare la motivazione alla base della decisione assunta e di giustificare la scelta del momento in cui fornire le informazioni. In pratica, può essere difficile adempiere tali obblighi quando si forniscono informazioni all'"ultimo momento". A tale proposito, il considerando 39 precisa, tra l'altro, che le persone interessate dovrebbero essere *"sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento"*. Il considerando 60 fa anch'esso riferimento al fatto che, nel contesto dei principi di trattamento corretto e trasparente, l'interessato dev'essere informato dell'esistenza del trattamento e delle sue finalità. Per tutti questi motivi, la posizione del Gruppo è che, conformemente al principio di correttezza, il titolare del trattamento dovrebbe ove possibile fornire le informazioni all'interessato con largo anticipo rispetto ai limiti di tempo previsti. I paragrafi 30, 31 e 48 riportano ulteriori considerazioni sull'adeguatezza del periodo che intercorre tra la comunicazione del trattamento agli interessati e il momento in cui il trattamento avviene.

Modifiche delle informazioni di cui agli articoli 13 e 14

29. La responsabilizzazione con riferimento alla trasparenza si applica non solo al momento della raccolta dei dati personali ma nell'intero ciclo di vita del trattamento, a prescindere dal fatto che le informazioni o le comunicazioni siano trasmesse. È questo il caso, ad esempio, quando si modificano i contenuti di dichiarazioni/informative sulla privacy esistenti. Il titolare del trattamento dovrebbe attenersi agli stessi principi quando comunica la dichiarazione/informativa sulla privacy iniziale e quando

comunica le modifiche materiali o sostanziali della stessa. I fattori di cui il titolare del trattamento dovrebbe tenere conto nel valutare che cosa si intenda per modifica materiale o sostanziale includono l'impatto sugli interessati (inclusa la loro capacità di esercitare i diritti di cui godono) e il carattere inatteso/sorprendente della modifica per gli stessi. Le modifiche della dichiarazione/informativa sulla privacy che dovrebbero essere sempre comunicate agli interessati comprendono la modifica della finalità del trattamento, la modifica dell'identità del titolare del trattamento e la modifica del modo in cui gli interessati possono esercitare i diritti di cui godono in relazione al trattamento. Per contro, la modifica di una dichiarazione/informativa sulla privacy che il Gruppo non ritiene essere materiale o sostanziale è, ad esempio, la correzione di un refuso o di un'imprecisione sintattica/grammaticale. Dal momento che la maggior parte dei clienti o utenti si limita a dare una rapida occhiata alle comunicazioni relative alle modifiche della dichiarazione/informativa sulla privacy, il titolare del cambiamento dovrebbe adottare tutte le misure necessarie per garantire che tali modifiche siano comunicate in modo tale da essere effettivamente notate dalla maggior parte dei destinatari. Ciò significa, ad esempio, che la modifica dovrebbe essere sempre comunicata in una modalità appropriata (ad es. e-mail, lettera scritta, finestra pop-up su una pagina Internet o altro modo che attiri efficacemente l'attenzione dell'interessato) specificamente dedicata alla modifica (ad es. non assieme a contenuti di commercializzazione diretta); inoltre, la comunicazione dovrebbe soddisfare i requisiti di cui all'articolo 12 di una forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. I riferimenti contenuti nella dichiarazione/informativa sulla privacy secondo cui l'interessato dovrebbe regolarmente controllarla per verificare la presenza di modifiche o aggiornamenti sono considerati non solo insufficienti, ma anche non corretti nel contesto dell'articolo 5, paragrafo 1, lettera a). Ulteriori orientamenti sulla tempistica per la comunicazione delle modifiche agli interessati figurano ai paragrafi 30 e 31.

Tempistica della comunicazione delle modifiche delle informazioni di cui agli articoli 13 e 14

30. Il regolamento non si esprime sui requisiti temporali (né sui metodi) che si applicano alla comunicazione delle modifiche delle informazioni precedentemente fornite all'interessato ai sensi dell'articolo 13 o 14 (escludendo un'ulteriore finalità prevista per il trattamento, nel qual caso, conformemente all'articolo 13, paragrafo 3, e all'articolo 14, paragrafo 4, le corrispondenti informazioni devono essere comunicate prima di iniziare l'ulteriore trattamento - si veda il paragrafo 45). Tuttavia, come sopra evidenziato nel contesto della tempistica per la fornitura d'informazioni di cui all'articolo 14, il titolare del trattamento deve tenere nuovamente conto dei principi di correttezza e responsabilizzazione, in termini di ragionevoli aspettative dell'interessato o di potenziale impatto della modifica sullo stesso. Se la modifica apportata alle informazioni è indicativa di un cambiamento fondamentale della natura del trattamento (ad es. am-

pliamento delle categorie di destinatari o introduzione di trasferimenti a un paese terzo) o di un cambiamento che, senza essere necessariamente fondamentale in termini di trattamento, può avere rilevanza e impatto sull'interessato, le informazioni in tal senso dovrebbero essere fornite all'interessato con largo anticipo sull'effettiva efficacia della modifica e il metodo utilizzato per segnalare la modifica all'interessato dovrebbe essere esplicito ed efficace. L'obiettivo è che l'interessato non si "perda" la modifica e che disponga di un termine ragionevole per a) valutare la natura e l'impatto della modifica e b) esercitare i diritti di cui gode in virtù del regolamento in relazione alla modifica stessa (ad es., revoca del consenso od opposizione al trattamento).

31. Il titolare del trattamento dovrebbe valutare con attenzione le circostanze e il contesto di ogni situazione qualora si renda necessario un aggiornamento delle informazioni finalizzate alla trasparenza, considerando tra l'altro il potenziale impatto delle modifiche sull'interessato e la modalità utilizzata per comunicarle, ed essere in grado di dimostrare che il periodo intercorso tra la comunicazione delle modifiche e la loro efficacia rispetta il principio di correttezza nei confronti dell'interessato. Inoltre, la posizione del Gruppo è che, coerentemente con il principio di correttezza, nel comunicare le modifiche agli interessati il titolare del trattamento debba anche spiegare quale sarà il probabile impatto su di essi. In ogni caso, la conformità ai requisiti di trasparenza non "sdogana" la situazione in cui le modifiche apportate al trattamento sono a tal punto rilevanti da snaturarlo. Il Gruppo sottolinea che tutte le altre norme del regolamento, incluse quelle relative all'ulteriore trattamento incompatibile, continuano a trovare applicazione a prescindere dalla conformità agli obblighi di trasparenza.

32. Anche quando le informazioni finalizzate alla trasparenza (ad es. contenute in una dichiarazione/informativa sulla privacy) non cambiano sostanzialmente, è probabile che gli interessati che utilizzano un servizio da molto tempo non rammentino le informazioni loro fornite all'inizio a norma dell'articolo 13 e/o 14. Il Gruppo raccomanda al titolare del trattamento di agevolare agli interessati un facile accesso continuativo alle informazioni, così che possano riacquisire familiarità con la portata del trattamento dei dati. Secondo il principio di responsabilizzazione, il titolare del trattamento dovrebbe valutare anche se, e a quali intervalli, sia appropriato inviare un promemoria esplicito agli interessati riguardo alla dichiarazione/informativa sulla privacy e al luogo in cui trovarla.

Modalità e formato della fornitura delle informazioni

33. Gli articoli 13 e 14 si riferiscono entrambi all'obbligo del titolare del trattamento, il quale *"fornisce all'interessato [...] le seguenti informazioni..."*. Il termine operativo è qui "fornisce". Ciò significa che il titolare del trattamento deve attivarsi per fornire le informazioni in questione all'interessato o per indirizzarlo verso il punto in cui si trovano (ad es. mediante link diretto, uti-

lizzo di un codice QR, ecc.). L'interessato non dev'essere costretto a cercare le informazioni contemplate in questi articoli tra le altre, come ad esempio fra le condizioni generali d'uso di un sito Internet o un'app. L'esempio riportato al paragrafo 11 illustra il punto. Come precisato al paragrafo 17, il Gruppo raccomanda che tutte le informazioni rivolte agli interessati siano messe a loro disposizione in un unico luogo o in un unico documento completo (ad es., in formato digitale su un sito Internet o su supporto cartaceo) cui si possa accedere facilmente per consultarle nella loro interezza.

34. Nel regolamento è insita una tensione tra, da un lato, l'obbligo di fornire agli interessati le necessarie informazioni complete e, dall'altro, l'obbligo di fornirle in una forma concisa, trasparente, intelligibile e facilmente accessibile. Tenuto conto dei principi fondamentali di responsabilizzazione e correttezza, il titolare del trattamento deve procedere quindi ad una propria analisi della natura, delle circostanze, della portata e del contesto del trattamento dei dati personali svolto e decidere, nell'ambito degli obblighi giuridici imposti dal regolamento e tenendo conto delle raccomandazioni contenute nelle presenti linee guida, in particolare al paragrafo 36, quale priorità assegnare alle informazioni da fornire agli interessati e quali livelli di dettaglio e metodi siano appropriati per trasmetterle.

Stratificazione in ambiente digitale e dichiarazioni/informative sulla privacy stratificate

35. Alla luce della quantità d'informazioni da fornire all'interessato, in ambiente digitale il titolare del trattamento può seguire un approccio stratificato, optando per una combinazione di metodi al fine di assicurare la trasparenza. Per evitare un subissamento informativo, il Gruppo raccomanda in particolare l'impiego di dichiarazioni/informative sulla privacy stratificate per collegare le varie categorie d'informazioni da fornire all'interessato, piuttosto che l'inserimento di tutte le informazioni in un'unica informativa sulla schermata. L'approccio stratificato può aiutare a superare la tensione tra completezza e comprensione, nello specifico consentendo agli utenti di muoversi direttamente verso la sezione della dichiarazione/informativa che vogliono leggere. Va notato che le dichiarazioni/informative sulla privacy non sono mere pagine annidiate in altre che richiedono diversi clic per arrivare all'informazione voluta: il design e il layout del primo strato della dichiarazione/informativa sulla privacy dovrebbe essere tale da offrire all'interessato una panoramica chiara delle informazioni a sua disposizione sul trattamento dei dati personali e del luogo e del modo in cui può trovarle fra i diversi strati. Un altro aspetto importante è la coerenza delle informazioni sia fra i diversi strati di una siffatta informativa sia all'interno di ogni singolo strato.

36. Con riferimento al contenuto della prima modalità utilizzata dal titolare del trattamento per informare gli interessati in un approccio stratificato (in altre parole, il metodo principale con cui il titolare si rivolge all'interessato) o al contenuto del primo strato della dichiarazione/informativa sulla

privacy stratificata, il Gruppo raccomanda che il primo strato/la prima modalità comprenda i dettagli delle finalità del trattamento, l'identità del titolare e una descrizione dei diritti dell'interessato (le informazioni dovrebbero inoltre essere portate direttamente all'attenzione dell'interessato nel momento della raccolta dei dati personali, vale a dire visualizzate quando l'interessato compila il modulo online).
L'importanza di fornire tali informazioni in anticipo deriva in particolare dal considerando 39[34]. Mentre i titolari del trattamento devono essere in grado di dar prova di responsabilizzazione per quanto concerne le ulteriori informazioni cui decidono di assegnare priorità, la posizione del Gruppo è che, in linea con il principio di correttezza, oltre alle informazioni indicate nel presente paragrafo il primo strato/la prima modalità debba contenere anche quelle relative al trattamento che ha il maggiore impatto sull'interessato e al trattamento che potrebbe coglierlo di sorpresa. Pertanto, l'interessato dovrebbe essere in grado di comprendere dalle informazioni contenute nel primo strato/nella prima modalità quali saranno per lui le conseguenze del trattamento (si veda anche il paragrafo 10).

37. In ambiente digitale, al di là della dichiarazione/informativa sulla privacy stratificata online il titolare del trattamento potrebbe anche scegliere di utilizzare altri strumenti di trasparenza (si vedano gli esempi sotto riportati) che forniscano all'interessato informazioni ad hoc specifiche per la sua situazione e per i beni/servizi di cui si avvale. Va tuttavia osservato che, mentre il Gruppo raccomanda l'utilizzo di dichiarazioni/informative sulla privacy stratificate online, la raccomandazione non esclude lo sviluppo e l'impiego di altri metodi innovativi di conformità agli obblighi di trasparenza.

Approccio stratificato in ambiente non digitale

38. Un approccio stratificato alla fornitura all'interessato delle informazioni finalizzate alla trasparenza è possibile anche in ambiente offline/non digitale (ad esempio nel mondo reale, come nella comunicazione telefonica o con presenza fisica degli interlocutori), nel quale il titolare del trattamento può scegliere fra varie modalità per facilitare la fornitura delle informazioni (si vedano anche i paragrafi da 33 a 37, 39 e 40 relativamente alle diverse modalità di fornire le informazioni). Quest'approccio non dev'essere confuso con la questione distinta delle dichiarazioni/informative sulla privacy stratificate. Quale che sia il formato utilizzato in quest'approccio stratificato, il Gruppo raccomanda che il primo "strato" (in altre parole, la modalità principale con cui il titolare del trattamento si rivolge inizialmente all'interessato) trasmetta di regola le informazioni più importanti (come indicato al paragrafo 36), vale a dire le finalità del trattamento, l'identità del titolare e una descrizione dei diritti dell'interessato, oltre a informazioni sull'impatto più consistente del trattamento o informazioni sul trattamento che potrebbe cogliere di sorpresa l'interessato. Ad esempio, se il primo contatto con l'interessato avviene telefonicamente, le informazioni potrebbero essere fornite durante la chiamata e, all'insegna

del bilanciamento delle informazioni richieste agli articoli 13 e 14, potrebbero essere comunicate con un ulteriore mezzo diverso, ad esempio inviando all'interessato una copia dell'informativa sulla privacy via e-mail e/o un link alla dichiarazione/informativa sulla privacy stratificata online del titolare del trattamento.

Notifiche "push" e "pull"

39. Un altro possibile modo per fornire informazioni finalizzate alla trasparenza è attraverso l'uso di notifiche "push" e "pull". Le notifiche "push" implicano la fornitura di messaggi "just in time", mentre quelle "pull" facilitano l'accesso alle informazioni con metodi quali la gestione dei permessi, dashboard per la privacy e tutorial per saperne di più. L'interessato può così fruire di un'esperienza maggiormente incentrata sull'utente.

    - Una dashboard per la privacy è un punto unico dal quale l'interessato può visualizzare le "informazioni sulla privacy" e gestire le proprie preferenze permettendo o impedendo al servizio in questione determinati usi dei dati che lo riguardano. È particolarmente utile quando l'interessato usa lo stesso servizio su diversi dispositivi, perché dà accesso ai dati personali e la possibilità di controllarli a prescindere dall'uso fatto del servizio. Il fatto che l'interessato possa modificare manualmente le impostazioni sulla privacy tramite un'apposita dashboard può inoltre facilitare la personalizzazione della dichiarazione/informativa sulla privacy, che sarà in grado di rispecchiare solo i tipi di trattamento che si verificano per quel particolare interessato. È preferibile incorporare una dashboard per la privacy nell'architettura preesistente di un servizio (ad es. con lo stesso design e branding del resto), perché questo favorirà l'intuitività dell'accesso e dell'uso e potrà contribuire a incoraggiare gli utenti a servirsi di queste informazioni, esattamente come farebbero con altre componenti del servizio. Può essere un modo efficace di dimostrare che le "informazioni sulla privacy" costituiscono un elemento necessario e parte integrante di un servizio anziché un lungo elenco di termini legalistici.

    - La notifica just-in-time è utilizzata per fornire "informazioni sulla privacy" specifiche in maniera ad hoc, vale a dire come e quando è più importante per l'interessato leggerle. Questo metodo è utile per fornire informazioni in vari momenti del processo di raccolta dei dati, favorisce una fornitura delle informazioni a blocchi assorbibili facilmente e riduce l'affidamento su un'unica dichiarazione/informativa sulla privacy piena d'informazioni difficilmente comprensibili fuori contesto. Ad esempio, se l'interessato acquista un prodotto online, possono essere fornite brevi informazioni esplicative in pop-up che accompagnano le pertinenti sezioni del testo. Accanto al campo che chiede il numero di telefono dell'interessato, le informazioni potrebbero ad esempio spiegare che il dato è raccolto soltanto per disporre di un contatto con riferimento all'acquisto e che sarà comunicato solo agli addetti del servizio di consegna.

Altri tipi di "misure appropriate"

40. Considerato il livello molto elevato di accesso a Internet nell'UE e il fatto che gli interessati possono collegarsi online in qualsiasi momento, da molteplici luoghi e da diversi dispositivi (come illustrato sopra), il Gruppo ritiene che, nel caso dei titolari del trattamento che hanno una presenza digitale/online, una "misura appropriata" per fornire informazioni finalizzate alla trasparenza è fornirle mediante una dichiarazione/informativa sulla privacy elettronica. In funzione delle circostanze della raccolta e del trattamento dei dati, il titolare del trattamento potrebbe tuttavia dover far uso di altre modalità e forme in aggiunta a detto metodo (o in alternativa ad esso, se non ha una presenza digitale/online). Altri modi possibili per trasmettere le informazioni all'interessato in funzione dei diversi ambienti dei dati personali possono includere le modalità di seguito elencate, applicabili al rispettivo ambiente. Come precedentemente osservato, il titolare del trattamento può adottare un approccio stratificato optando per una combinazione di tali metodi e garantendo al contempo che le informazioni più importanti (si vedano i paragrafi 36 e 38) siano sempre trasmesse nella prima modalità usata per comunicare con l'interessato.

    a. Ambiente cartaceo, ad esempio quando si stipulano contratti per via postale: spiegazioni scritte, opuscoli, informazioni contenute nella documentazione contrattuale, vignette, infografica o diagrammi.
    b. Ambiente telefonico: spiegazioni orali date da una persona in carne e ossa, per consentire l'interazione e risposte alle domande, oppure informazioni automatiche o preregistrate con opzioni per ascoltare altre informazioni più dettagliate.
    c. Tecnologia smart senza schermo/ambiente IoT come analisi del tracciamento Wi-Fi: icone, codici QR, notifiche vocali, dettagli scritti incorporati in istruzioni di set-up cartacee, video incorporati in istruzioni di set-up digitali, informazioni scritte sul dispositivo smart, messaggi inviati via SMS o e-mail, pannelli visibili contenenti informazioni, segnaletica o campagne pubbliche d'informazione.
    d. Ambiente interpersonale, come la risposta a sondaggi di opinione, la registrazione di persona per un servizio: spiegazioni orali o scritte fornite in forma cartacea o digitale.
    e. Ambiente di "vita reale" con registrazione CCTV/ tramite drone: pannelli visibili contenenti informazioni, segnaletica pubblica, campagne pubbliche d'informazione o avvisi sui giornali/media.

Informazioni sulla profilazione e sul processo decisionale automatizzato

41. Nelle informazioni obbligatorie da fornire all'interessato ai sensi dell'articolo 13, paragrafo 2, lettera f), e dell'articolo 14, paragrafo 2, lettera g), rientrano le informazioni sull'esistenza di un processo decisionale automatizzato, comprensivo della profilazione, quale previsto all'articolo 22, paragrafi 1 e 4, unitamente a informazioni pregnanti sulla logica applicata e le conseguenze rilevanti che si prevede il trattamento avrà per l'interes-

sato. Il Gruppo ha elaborato linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione[35], cui si dovrebbe fare riferimento per un ulteriore orientamento sul modo in cui attuare la trasparenza nelle particolari circostanze della profilazione. Va notato che, a parte gli specifici obblighi di trasparenza applicabili al processo decisionale automatizzato di cui all'articolo 13, paragrafo 2, lettera f), e all'articolo 14, paragrafo 2, lettera g), le considerazioni contenute nelle presenti linee guida relativamente all'importanza d'informare gli interessati delle conseguenze del trattamento dei dati personali che li riguardano e il principio generale secondo cui questo trattamento non dovrebbe cogliere di sorpresa l'interessato si applicano parimenti alla profilazione in generale (non solo a quella descritta all'articolo 22[36]) in quanto tipologia di trattamento[37].

Altre questioni – rischi, norme e garanzie

42. Il considerando 39 del regolamento fa riferimento alla fornitura di determinate informazioni non esplicitamente trattate dagli articoli 13 e 14 (si veda il testo del considerando riportato al paragrafo 28). Il riferimento alla sensibilizzazione degli interessati ai rischi, alle norme e alle garanzie relativi al trattamento dei dati personali è connesso a varie altre questioni, che includono le valutazioni d'impatto sulla protezione dei dati. Come stabilito nelle linee guida del Gruppo in materia di valutazione d'impatto sulla protezione dei dati[38], benché non esista un obbligo in tal senso il titolare del trattamento può vagliare l'ipotesi di pubblicare la valutazione d'impatto sulla protezione dei dati (o una sua parte) come modo per iniettare fiducia nei trattamenti effettuati e dar prova di responsabilizzazione e trasparenza. Per dar prova di trasparenza può inoltre risultare utile il rispetto di un codice di condotta (previsto all'articolo 40), dal momento che è possibile predisporre codici di condotta allo scopo di specificare alcuni aspetti dell'applicazione del regolamento, quali trattamento corretto e trasparente, informazioni fornite al pubblico e agli interessati e informazioni fornite ai minori e tutela degli stessi.

43. Un altro aspetto rilevante riguardo alla trasparenza è la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita (previste all'articolo 25). Questi principi impongono al titolare di integrare le considerazioni sulla protezione dei dati nelle operazioni e nei sistemi di trattamento fin dalla fase iniziale, anziché considerare la protezione dei dati una questione di conformità di cui occuparsi all'ultimo minuto. Il considerando 78 si riferisce ai titolari del trattamento che attuano misure che soddisfano i requisiti della protezione dei dati fin dalla progettazione e per impostazione predefinita, tra cui misure di trasparenza con riferimento alle funzioni e al trattamento dei dati personali.

44. La questione distinta dei contitolari del trattamento è anch'essa connessa alla sensibilizzazione degli interessati ai rischi, alle norme e alle garanzie. L'articolo 26, paragrafo 1, impone ai contitolari di determinare le rispet-

tive responsabilità di ciascuno in merito all'osservanza degli obblighi derivanti dal regolamento in maniera trasparente, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14. L'articolo 26, paragrafo 2, prescrive che il contenuto essenziale dell'accordo tra i titolari del trattamento debba essere messo a disposizione dell'interessato. In altre parole, dev'essere completamente chiaro all'interessato a quale titolare debba rivolgersi qualora intenda esercitare uno o più dei diritti che gli spettano ai sensi del regolamento[39].

INFORMAZIONI RELATIVE ALL'ULTERIORE TRATTAMENTO

45. Gli articoli 13 e 14 contengono entrambi una disposizione[40] che impone al titolare del trattamento d'informare l'interessato qualora intenda trattare ulteriormente i dati personali che lo riguardano per una finalità diversa da quella per cui sono stati raccolti/ottenuti. In tal caso, "prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2". Tali disposizioni danno concreta attuazione al principio di cui all'articolo 5, paragrafo 1, lettera b), secondo cui i dati personali devono essere raccolti per finalità determinate, esplicite e legittime ed è vietato trattarli successivamente in modo incompatibile con tali finalità[41]. La seconda parte dell'articolo 5, paragrafo 1, lettera b), afferma che un ulteriore trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali. Qualora i dati personali siano ulteriormente trattati per finalità compatibili con quelle iniziali (l'articolo 6, paragrafo 4, regola la questione[42]), trovano applicazione l'articolo 13, paragrafo 3, e l'articolo 14, paragrafo 4. Le disposizioni di questi articoli che impongono di informare l'interessato dell'ulteriore trattamento supportano la posizione assunta nel regolamento, secondo cui l'interessato dovrebbe ragionevolmente attendersi, al momento e nel contesto della raccolta dei dati personali, che possa avere luogo un trattamento per una particolare finalità[43]. In altre parole, l'interessato non dovrebbe essere colto di sorpresa dalla finalità del trattamento dei dati personali che lo riguardano.

46. Nella parte in cui si riferiscono alla fornitura di *"ogni ulteriore informazione pertinente di cui al paragrafo 2"*, l'articolo 13, paragrafo 3, e l'articolo 14, paragrafo 4, possono essere interpretati a prima vista come se lasciassero al titolare del trattamento una certa libertà di valutazione circa la portata e le categorie particolari d'informazioni di cui al rispettivo paragrafo 2 (ovvero, a seconda del caso, articolo 13, paragrafo 2, o articolo 14, paragrafo 2) che dovrebbero essere fornite all'interessato (il considerando 61 parla a tale proposito di *"altre informazioni necessarie"*). La posizione prestabilita è comunque che tutte le informazioni di cui a detto paragrafo dovrebbero essere fornite all'interessato, salvo che una o più categorie d'informazioni non esistano o non siano applicabili.

47. Il Gruppo raccomanda che i titolari del trattamento, per essere trasparenti, corretti e responsabili, considerino di mettere a disposizione degli interessati, nella rispettiva dichiarazione/informativa sulla privacy, informazioni sull'analisi di compatibilità svolta ai sensi dell'articolo 6, paragrafo 4[44], qualora la nuova finalità del trattamento si fondi su una base giuridica diversa dal consenso o da un atto legislativo dell'Unione o degli Stati membri (in altre parole, una spiegazione del modo in cui il trattamento per una finalità diversa sia compatibile con la finalità iniziale). L'intento è offrire agli interessati la possibilità di valutare la compatibilità dell'ulteriore trattamento e delle garanzie fornite e di decidere se esercitare o no i loro diritti, ad es., tra gli altri, il diritto di limitazione di trattamento o il diritto di opporsi al trattamento[45]. Laddove i titolari del trattamento scelgano di non includere tali informazioni nella dichiarazione/informativa sulla privacy, il Gruppo raccomanda che esplicitino agli interessati il fatto che tali informazioni possono essere ottenute su richiesta.

48. Connessa all'esercizio dei diritti dell'interessato è la questione della tempestività. Come evidenziato sopra, la fornitura d'informazioni in maniera tempestiva è un elemento di vitale importanza degli obblighi di trasparenza di cui agli articoli 13 e 14, intrinsecamente legato al concetto di trattamento corretto. Le informazioni relative all'ulteriore trattamento devono essere fornite "prima di tale ulteriore trattamento". Il Gruppo ritiene che tra la comunicazione e l'inizio del trattamento debba intercorrere un periodo di tempo ragionevole, e non che il trattamento cominci non appena l'interessato riceve la comunicazione. Ciò garantisce agli interessati i vantaggi pratici del principio della trasparenza, offrendo loro una possibilità significativa di valutare l'ulteriore trattamento (e potenzialmente esercitare i loro diritti al riguardo). Quale sia un termine ragionevole dipende dalle circostanze specifiche. Il principio della correttezza impone che più invasivo (o meno atteso) è l'ulteriore trattamento, più lungo debba essere il periodo. Allo stesso modo, il principio di responsabilizzazione implica che i titolari del trattamento siano in grado di dimostrare che le conclusioni cui sono giunti circa la tempistica della fornitura delle informazioni sono giustificate nel caso specifico e che la tempistica è nel complesso corretta nei confronti degli interessati (si vedano anche le precedenti considerazioni circa la valutazione dei termini ragionevoli ai paragrafi 30-32.)

STRUMENTI DI VISUALIZZAZIONE

49. Un aspetto importante è che nel regolamento l'attuazione del principio della trasparenza non si limita alle comunicazioni linguistiche (siano essere scritte od orali). Il regolamento prevede, se del caso, il ricorso a strumenti di visualizzazione (con particolare riferimento a icone, meccanismi di certificazione, sigilli e marchi di protezione dei dati). Il considerando 58[46] indica che l'accessibilità delle informazioni rivolte al pubblico o agli interessati è particolarmente importante nell'ambiente online[47].

Icone

50. Il considerando 60 prevede che le informazioni siano fornite all'interessato "in combinazione" con icone standardizzate, ammettendo così un approccio stratificato. Le icone non dovrebbero tuttavia essere usate come semplice sostituto delle informazioni necessarie per l'esercizio dei diritti dell'interessato né come sostituto per assicurare la conformità agli obblighi del titolare del trattamento previsti agli articoli 13 e 14. L'articolo 12, paragrafo 7, prevede l'uso di tale icone affermando che:

> *"Le informazioni da fornire agli interessati a norma degli articoli 13 e 14 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico".*

51. Dal momento che l'articolo 12, paragrafo 7, afferma che *"[s]e presentate elettronicamente, le icone sono leggibili da dispositivo automatico"*, possono esserci situazioni in cui le icone non sono presentate elettronicamente[48], ma sono, ad esempio, icone riportate su materiale cartaceo, dispositivi IoT oppure su imballaggi di dispositivi IoT, avvisi in luoghi pubblici riguardo al tracciamento Wi-Fi, codici QR e notifiche CCTV.

52. È evidente che le icone sono utilizzate allo scopo di aumentare la trasparenza per gli interessati, in quanto presentano la potenzialità di ridurre la necessità di presentare loro grandi quantità d'informazioni scritte. A ogni modo, l'utilità delle icone per trasmettere in maniera efficace agli interessati le informazioni richieste dagli articoli 13 e 14 dipende dalla standardizzazione dei simboli/delle immagini, che dovrebbero essere di uso universale e riconosciuti in tutta l'UE come rappresentazione schematica dell'informazione corrispondente. A tale riguardo, il regolamento attribuisce alla Commissione la responsabilità dello sviluppo di un codice iconografico, ma in definitiva il comitato europeo per la protezione dei dati può, su richiesta della Commissione o di propria iniziativa, fornire alla Commissione un parere in merito a dette icone[49]. Il Gruppo riconosce che, in linea con il considerando 166, lo sviluppo di un codice iconografico dovrebbe basarsi su un approccio empirico e che, prima di una simile standardizzazione, sarà necessario condurre, in collaborazione con gli operatori del settore e il pubblico in generale, estese ricerche sull'efficacia delle icone in questo contesto.

Meccanismi di certificazione, sigilli e marchi

53. Oltre alle icone standardizzate, il regolamento (articolo 42) prevede anche l'uso di meccanismi di certificazione della protezione dei dati, nonché di sigilli e marchi di protezione dei dati, allo scopo di dimostrare la conformità al regolamento dei trattamenti effettuati dai titolari del trattamento

e dai responsabili del trattamento e migliorare la trasparenza per gli interessati[50]. Il Gruppo pubblicherà a tempo debito linee guida sui meccanismi di certificazione.

ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

54. La trasparenza impone al titolare del trattamento un triplice obbligo per quanto attiene ai diritti dell'interessato previsti dal regolamento, dal momento che deve[51]:

    - fornire informazioni agli interessati sui loro diritti[52] (come previsto all'articolo 13, paragrafo, 2, lettera b), e all'articolo 14, paragrafo 2, lettera c));
    - rispettare il principio di trasparenza (relativamente alla qualità delle comunicazioni, come stabilito all'articolo 12, paragrafo 1) nella comunicazione con gli interessati riguardo all'esercizio dei loro diritti ai sensi degli articoli 15-22 e dell'articolo 34;
    - agevolare l'esercizio dei diritti degli interessati ai sensi degli articoli 15-22.

55. Gli obblighi imposti dal regolamento in relazione all'esercizio di tali diritti e alla natura delle informazioni necessarie mirano a posizionare adeguatamente gli interessati in modo che possano rivendicare i loro diritti e ritenere i titolari del trattamento responsabili del trattamento dei dati personali che li riguardano. Il considerando 59 precisa che *"[è] opportuno prevedere modalità volte ad agevolare l'esercizio, da parte dell'interessato, dei diritti"* e che i titolari del trattamento dovrebbero *"predisporre anche i mezzi per inoltrare le richieste per via elettronica, in particolare qualora i dati personali siano trattati con mezzi elettronici"*. La modalità che il titolare del trattamento offre all'interessato per l'esercizio dei suoi diritti dovrebbe essere appropriata al contesto e alla natura del rapporto e delle interazioni tra loro. A tal fine, può risultare utile al titolare del trattamento offrire una o più modalità diverse che rispecchino i diversi modi in cui interagisce con l'interessato.

Esempio

Un fornitore di servizi sanitari utilizza un modulo elettronico sul proprio sito Internet e moduli cartacei alla reception delle sue cliniche per facilitare l'inoltro di richieste di accesso ai dati personali, online e di persona. Pur offrendo queste modalità, il fornitore di servizi sanitari accetta anche richieste di accesso presentate in altri modi (ad esempio via lettera o e-mail) e mette a disposizione un ufficio dedicato (accessibile via e-mail o telefonicamente) per assistere gli interessati nell'esercizio dei loro diritti.

ECCEZIONI ALL'OBBLIGO DI FORNIRE INFORMAZIONI

Eccezioni all'articolo 13

56. La sola eccezione agli obblighi del titolare del trattamento di cui all'articolo 13, qualora abbia raccolto dati personali direttamente presso l'interessato, si ha *"se e nella misura in cui l'interessato dispone già delle informazioni"*[53]. Il principio di responsabilizzazione impone al titolare del trattamento di dimostrare (e documentare) quali informazioni l'interessato possiede già, come e quando le ha ricevute e l'assenza di modifiche delle informazioni tali da renderle obsolete. Inoltre, l'espressione "nella misura in cui" all'articolo 13, paragrafo 4, chiarisce che, anche se all'interessato sono state precedentemente fornite determinate categorie d'informazioni fra quelle previste all'articolo 13, sussiste comunque, in capo al titolare del trattamento, l'obbligo di integrarle per garantire che l'interessato disponga di un insieme completo delle informazioni elencate all'articolo 13, paragrafi 1 e 2. Segue un esempio di migliore prassi relativamente al modo restrittivo in cui andrebbe interpretata l'eccezione prevista all'articolo 13, paragrafo 4.

Esempio

Una persona sottoscrive un servizio di posta elettronica online e riceve tutte le informazioni richieste dall'articolo 13, paragrafi 1 e 2, al momento della sottoscrizione. Sei mesi dopo l'interessato attiva una funzione di messaggeria istantanea tramite il fornitore del servizio di posta elettronica e a tal fine comunica il proprio numero di cellulare. Il fornitore del servizio trasmette all'interessato alcune informazioni di cui all'articolo 13, paragrafi 1 e 2, riguardo al trattamento del numero di telefono (ad es. finalità e base giuridica del trattamento, destinatari, periodo di conservazione), ma omette di fornirne altre di cui la persona è già in possesso da 6 mesi e che da allora non sono cambiate (ad es. l'identità e i dati di contatto del titolare e del responsabile della protezione dei dati, informazioni sui diritti dell'interessato e sul diritto di proporre reclamo all'autorità di controllo competente). La migliore prassi richiede tuttavia che all'interessato sia nuovamente fornito il pacchetto completo d'informazioni, ma che sia in grado di individuare con facilità le novità rispetto al passato. Il nuovo

trattamento per la finalità del servizio di messaggeria istantanea potrebbe incidere sull'interessato a tal punto da indurlo a esercitare un diritto di cui potrebbe essersi dimenticato, avendo ricevuto le informazioni sei mesi prima. Fornire di nuovo tutte le informazioni contribuisce a garantire che l'interessato rimanga adeguatamente informato sul modo in cui sono utilizzati i dati che lo riguardano e sui diritti di cui gode.

Eccezioni all'articolo 14

57. Se i dati personali non sono stati ottenuti presso l'interessato, l'articolo 14 prevede una serie molto più ampia di eccezioni all'obbligo d'informazione incombente al titolare del trattamento. In linea generale, tali eccezioni dovrebbero essere interpretate e applicate restrittivamente. Oltre alle circostanze in cui l'interessato dispone già delle informazioni in questione (articolo 14, paragrafo 5, lettera a)), l'articolo 14, paragrafo 5, ammette le seguenti eccezioni:

    - comunicare le informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato, in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, o renderebbe impossibile o pregiudicherebbe gravemente il conseguimento delle finalità del trattamento;
    - l'ottenimento o la comunicazione dei dati personali sono previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare i legittimi interessi dell'interessato;
    - un obbligo di segreto professionale (incluso un obbligo di segretezza previsto per legge) disciplinato dal diritto dell'Unione o degli Stati membri implica che i dati personali devono rimanere riservati.

Impossibilità, sforzo sproporzionato e grave pregiudizio delle finalità

58. L'articolo 14, paragrafo 5, lettera b), prevede tre situazioni distinte in cui è fatta eccezione all'obbligo di fornire le informazioni di cui all'articolo 14, paragrafi 1, 2 e 4:

    (I) qualora ciò risulti impossibile (in particolare per il trattamento a fini di archiviazione, di ricerca scientifica o storica o a fini statistici);
    (II) qualora implichi uno sforzo sproporzionato (in particolare per il trattamento a fini di archiviazione, di ricerca scientifica o storica o a fini statistici);
    (III) qualora comunicare le informazioni richieste dall'articolo 14, paragrafo 1, rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità del trattamento.

"Risulta impossibile"

59. La situazione in cui la comunicazione delle informazioni "risulta impossibile" ai sensi dell'articolo 14, paragrafo 5, lettera b), è del tipo "bianco o

nero", perché una certa cosa è impossibile oppure non lo è: non esistono gradazioni di impossibilità. Pertanto, se intende valersi dell'eccezione, il titolare del trattamento deve dimostrare i fattori che effettivamente gli impediscono di fornire le informazioni all'interessato. Se, trascorso un certo periodo di tempo, i fattori che hanno determinato l'"impossibilità" svaniscono e la comunicazione delle informazioni all'interessato diventa possibile, il titolare del trattamento dovrebbe provvedervi immediatamente. In pratica, vi saranno pochissime situazioni in cui il titolare del trattamento potrà dimostrare l'effettiva impossibilità di fornire le informazioni all'interessato; l'esempio seguente lo dimostra.

Esempio

L'interessato si registra per un servizio di abbonamento online con pagamento a posteriori. Dopo la registrazione, il titolare del trattamento raccoglie dati relativi alla solvibilità dell'interessato da un'agenzia dedicata, al fine di decidere se fornire o no il servizio. Il protocollo del titolare del trattamento prevede che si informino gli interessati della raccolta di tali dati entro tre giorni, conformemente all'articolo 14, paragrafo 3, lettera a). Tuttavia, l'indirizzo e il numero di telefono dell'interessato non sono riportati nei pubblici registri (l'interessato vive all'estero). L'interessato non ha lasciato un indirizzo e-mail al momento della registrazione per il servizio o l'indirizzo e-mail fornito non è valido. Il titolare del trattamento ritiene di non avere mezzi per contattare direttamente l'interessato. In questo caso, comunque, il titolare del trattamento potrebbe fornire informazioni circa la raccolta dei dati sulla solvibilità sul proprio sito Internet, prima della registrazione. In tal modo non risulterebbe impossibile fornire le informazioni a norma dell'articolo 14.

Impossibilità di specificare la fonte dei dati

60. Il considerando 61 afferma che *"[q]ualora non sia possibile comunicare all'interessato l'origine dei dati personali, perché sono state utilizzate varie fonti, dovrebbe essere fornita un'informazione di carattere generale"*. L'esenzione dall'obbligo di fornire all'interessato informazioni sulla fonte dei dati personali che lo riguardano si applica solo se è impossibile attribuire a una determinata fonte i diversi dati personali ottenuti. Ad esempio, il mero fatto che il titolare del trattamento abbia compilato una banca dati contenente i dati personali di diversi interessati utilizzando più di una fonte non è sufficiente per derogare all'obbligo se è possibile (benché laborioso e dispendioso in termini di tempo) individuare la fonte a cui sono stati attinti i dati personali dei singoli interessati. Dato l'obbligo della protezione dei dati fin dalla progettazione e per impostazione predefinita[54], i meccanismi di trasparenza dovrebbero essere integrati nei sistemi di trattamento sin dall'inizio, in maniera tale da poter rintracciare tutte le fonti dei dati personali ricevuti in un'organizzazione e

da poter risalire ad esse in qualsiasi momento del ciclo di vita del trattamento (si veda il paragrafo 43).

"Sforzo sproporzionato"

61. Ai sensi dell'articolo 14, paragrafo 5, lettera b), oltre alla situazione di "impossibilità" può trovare applicazione lo "sforzo sproporzionato", in particolare per il trattamento *"a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1"*. Anche il considerando 62 si riferisce a queste finalità come a situazioni in cui informare l'interessato richiederebbe uno sforzo sproporzionato e afferma che, in tali casi, si dovrebbe tener conto del numero di interessati, dell'antichità dei dati e delle eventuali garanzie adeguate in essere. Considerato il rilievo posto dal considerando 62 e dall'articolo 14, paragrafo 5, lettera b), sulle finalità di archiviazione, di ricerca o statistiche, il Gruppo considera che, *nell'ordinario*, il titolare che non tratta dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non debba avvalersi di quest'esenzione. Il Gruppo sottolinea che, se queste sono le finalità perseguite, occorre soddisfare le condizioni di cui all'articolo 89, paragrafo 1, e che la comunicazione delle informazioni deve costituire uno sforzo sproporzionato.

62. Nel determinare che cosa possa configurare un'impossibilità o uno sforzo sproporzionato ai sensi dell'articolo 14, paragrafo 5, lettera b), è interessante rilevare che esenzioni analoghe non sono previste all'articolo 13 (se i dati personali sono raccolti presso l'interessato). L'unica differenza tra la situazione di cui all'articolo 13 e quella di cui all'articolo 14 è che, nella seconda, i dati personali non sono raccolti presso l'interessato. Ne consegue pertanto che l'impossibilità o lo sforzo sproporzionato deriva tipicamente da circostanze che non si applicano se i dati personali sono raccolti presso l'interessato. In altre parole, l'impossibilità o lo sforzo sproporzionato deve ricollegarsi direttamente al fatto che i dati personali sono stati ottenuti da fonte diversa dall'interessato.

Esempio

L'ospedale di una grande città chiede a tutti i pazienti che vi si recano per trattamenti in day-hospital, ricoveri di lunga durata o visite mediche di compilare un modulo di raccolta dati del paziente in cui occorre indicare gli estremi di due parenti stretti (gli interessati). Considerato l'enorme numero di pazienti che ogni giorno passano per l'ospedale, comunicare le informazioni di cui all'articolo 14 a tutte le persone elencate come parenti stretti sui moduli compilati dai pazienti richiederebbe uno sforzo sproporzionato da parte dell'ospedale.

63. I fattori richiamati nel considerando 62 (numero di interessati, antichità dei dati ed eventuali garanzie adeguate in essere) possono essere in-

dicativi dei tipi di questioni che contribuiscono a far sì che il titolare del trattamento debba compiere uno sforzo sproporzionato per comunicare all'interessato le informazioni di cui all'articolo 14.

Esempio

Alcuni storici conducono una ricerca intesa a ricostruire la genealogia in base ai cognomi; in tale contesto ottengono indirettamente una consistente serie di dati su 20 000 interessati. I dati sono tuttavia stati raccolti 50 anni prima, non sono più stati aggiornati da allora e non includono i dati di contatto. Considerata la mole di dati e, più particolarmente, l'antichità degli stessi, rintracciare gli interessati a uno a uno per fornire loro le informazioni di cui all'articolo 14 richiederebbe uno sforzo sproporzionato da parte dei ricercatori.

64. Qualora intenda avvalersi dell'eccezione di cui all'articolo 14, paragrafo 5, lettera b), perché la comunicazione delle informazioni implicherebbe uno sforzo sproporzionato, il titolare del trattamento dovrebbe effettuare una valutazione mettendo sulla bilancia, da un lato, lo sforzo che fornire le informazioni all'interessato gli implicherebbe e, dall'altro, l'impatto e gli effetti dell'omessa comunicazione sull'interessato. Il titolare del trattamento dovrebbe documentare tale valutazione conformemente agli obblighi di responsabilizzazione che gl'incombono. In siffatto caso, l'articolo 14, paragrafo 5, lettera b), precisa che il titolare deve adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato. Ciò si applica parimenti se il titolare del trattamento stabilisce che la comunicazione delle informazioni risulta impossibile oppure può rendere impossibile o pregiudicare gravemente il conseguimento delle finalità del trattamento. Come specificato all'articolo 14, paragrafo 5, lettera b), una delle misure appropriate che il titolare del trattamento deve adottare sempre è rendere pubbliche le informazioni. Questo è possibile in un certo numero di modi, ad esempio pubblicando le informazioni sul proprio sito Internet oppure pubblicizzandole proattivamente su un giornale o su manifesti nei propri locali. Le altre misure appropriate, oltre alla pubblicità delle informazioni, dipenderanno dalle circostanze del trattamento, ma potranno includere l'effettuazione di una valutazione d'impatto sulla protezione dei dati, l'applicazione di tecniche di pseudonimizzazione dei dati, la minimizzazione dei dati raccolti e del periodo di conservazione e l'attuazione di misure tecniche e organizzative finalizzate a un livello elevato di sicurezza. Vi possono inoltre essere situazioni in cui il titolare tratta dati personali che non richiedono l'identificazione dell'interessato (ad esempio dati pseudonimizzati). In tali casi, può risultare pertinente anche l'articolo 11, paragrafo 1, dal momento che afferma che il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il regolamento.

Grave pregiudizio delle finalità

65. L'ultima situazione contemplata dall'articolo 14, paragrafo 5, lettera b), è quella in cui la comunicazione all'interessato, da parte del titolare del trattamento, delle informazioni di cui all'articolo 14, paragrafo 1, potrebbe rendere impossibile o pregiudicare gravemente il conseguimento delle finalità del trattamento. Per avvalersi di quest'eccezione, il titolare del trattamento deve dimostrare che basterebbe fornire le informazioni di cui all'articolo 14, paragrafo 1, per vanificare le finalità del trattamento. Segnatamente, quest'aspetto dell'articolo 14, paragrafo 5, lettera b), può essere addotto presupponendo che il trattamento dei dati rispetti tutti i principi stabiliti all'articolo 5 e che, cosa ancor più importante, il trattamento dei dati personali sia corretto e abbia una base giuridica in tutte le circostanze.

Esempio

La normativa antiriciclaggio obbliga la banca A a segnalare alla competente autorità di polizia economico-finanziaria le operazioni sospette relative ai conti detenuti presso di essa. La banca A riceve dalla banca B (di un altro Stato membro) l'informazione che un dato correntista ha disposto il trasferimento di una certa somma a un altro conto detenuto presso la banca A, il che appare sospetto. La banca A trasmette i dati relativi al correntista e alle operazioni sospette alla competente autorità di polizia economico-finanziaria. Secondo la normativa antiriciclaggio in questione, commette reato la banca segnalatrice che, con una "soffiata", avvisa il correntista del fatto che potrebbe essere sottoposto a indagini a norma di legge. In tale situazione, l'articolo 14, paragrafo 5, lettera b), trova applicazione, dal momento che fornire all'interessato (il correntista della banca A) le informazioni di cui all'articolo 14 sul trattamento dei dati personali che lo riguardano, ricevuti dalla banca B, pregiudicherebbe gravemente le finalità della normativa, che include la prevenzione delle "soffiate". Tuttavia, all'apertura di un conto la banca A dovrebbe fornire a tutti i correntisti informazioni generali che indichino che i dati che li riguardano potranno essere trattati per finalità di antiriciclaggio.

Ottenimento o comunicazione d'informazioni espressamente previsti per legge

66. L'articolo 14, paragrafo 5, lettera c), ammette l'esenzione dagli obblighi d'informazione di cui all'articolo 14, paragrafi 1, 2 e 4, nella misura in cui l'ottenimento o la comunicazione dei dati personali *"sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento"*. L'esenzione è subordinata alla condizione che il diritto in questione preveda *"misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato"*. Il diritto in questione deve riguardare direttamente il titolare del trattamento, per il quale l'ottenimento o la comunicazione dovrebbero essere obbligatori. Di conseguenza, il titolare del trattamento

dev'essere in grado di dimostrare che il diritto in questione trova applicazione nei suoi confronti e gli impone l'ottenimento o la comunicazione dei dati personali. Sebbene spetti al diritto dell'Unione europea o dello Stato membro inquadrare la normativa in maniera tale che preveda *"misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato"*, il titolare del trattamento dovrebbe garantire (ed essere in grado di dimostrare) di aver ottenuto o comunicato i dati personali in conformità di tali misure. Salvo se la legge gli impedisce di agire in tal senso, il titolare del trattamento dovrebbe inoltre chiarire agli interessati che l'ottenimento o la comunicazione dei dati personali è conforme al diritto in questione. Ciò è in linea con il considerando 41 del regolamento, il quale afferma che una base giuridica o una misura legislativa dovrebbe essere chiara e precisa e la sua applicazione prevedibile per le persone che vi sono sottoposte, in conformità della giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo. Tuttavia, l'articolo 14, paragrafo 5, lettera c), non troverà applicazione qualora sussista per il titolare del trattamento l'obbligo di ottenere i dati *direttamente presso l'interessato*, nel qual caso si applicherà l'articolo 13. In tal caso, la sola eccezione prevista dal regolamento che esoneri il titolare del trattamento dal fornire all'interessato le informazioni sul trattamento sarà quella prevista all'articolo 13, paragrafo 4 (vale a dire se e nella misura in cui l'interessato dispone già delle informazioni). Come riportato al paragrafo 68, a livello nazionale gli Stati membri possono tuttavia legiferare, conformemente all'articolo 23, su ulteriori specifiche limitazioni del diritto alla trasparenza di cui all'articolo 12 e all'informazione ai sensi degli articoli 13 e 14.

Esempio

Un'autorità fiscale è soggetta all'obbligo, previsto dal diritto nazionale, di ottenere dai datori di lavoro dati sui salari dei dipendenti. I dati personali non sono ottenuti presso gli interessati e pertanto l'autorità fiscale è soggetta agli obblighi di cui all'articolo 14. Dal momento che questo tipo di ottenimento dei dati personali presso i datori di lavoro è espressamente previsto dalla legge, l'autorità fiscale non è sottoposta agli obblighi d'informazione di cui all'articolo 14.

Riservatezza a fronte di un obbligo di segretezza

67. L'articolo 14, paragrafo 5, lettera d), prevede un'esenzione dall'obbligo d'informazione in capo al titolare del trattamento qualora i dati personali *"debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri"*. Se intende avvalersi di quest'esenzione, il titolare del trattamento dev'essere in grado di provare di averla identificata in maniera appropriata e di mostrare come l'obbligo del segreto professionale lo riguardi direttamente al punto tale da impedirgli di fornire all'interessato tutte le informazioni di cui all'articolo 14, paragrafi 1, 2 e 4.

Esempio

Un medico (titolare del trattamento) è soggetto all'obbligo di segreto professionale per quanto concerne le informazioni mediche dei suoi pazienti. Una paziente (nei confronti della quale si applica l'obbligo di segreto professionale) fornisce al medico informazioni sul suo stato di salute relativamente a una condizione genetica che interessa anche un certo numero di suoi parenti stretti. La paziente fornisce al medico anche determinati dati personali dei parenti (gli interessati) che presentano la stessa condizione. Al medico non è imposto di fornire ai parenti le informazioni di cui all'articolo 14, dal momento che trova applicazione l'esenzione prevista all'articolo 14, paragrafo 5, lettera d). Se il medico dovesse fornire le informazioni di cui all'articolo 14 ai parenti, sarebbe violato l'obbligo di segreto professionale cui è soggetto nei confronti della paziente.

LIMITAZIONI DEI DIRITTI DEGLI INTERESSATI

68. L'articolo 23 prevede che gli Stati membri (o l'UE) legiferino su ulteriori limitazioni della portata dei diritti degli interessati relativi alla trasparenza e dei loro diritti sostanziali[55], nella misura in cui tali misure rispettino l'essenza dei diritti e delle libertà fondamentali e siano necessarie e proporzionate per salvaguardare una o più delle dieci finalità previste all'articolo 23, paragrafo 1, lettere da a) a j). Qualora tali misure nazionali limitino i diritti specifici degli interessati o gli obblighi generali di trasparenza che altrimenti si applicherebbero ai titolari del trattamento ai sensi del regolamento, questi ultimi dovrebbero essere in grado di dimostrare in che modo la norma nazionale si applichi loro. Come stabilito all'articolo 23, paragrafo 2, lettera h), la misura legislativa deve contenere una disposizione circa il diritto degli interessati di essere informati della limitazione, a meno che ciò possa comprometterne la finalità. Coerentemente, e in linea con il principio di correttezza, il titolare del trattamento dovrebbe informare l'interessato anche del fatto che si sta avvalendo (o si avvarrà nel caso in cui sia esercitato un particolare diritto dell'interessato) di una limitazione legislativa nazionale dell'esercizio dei diritti degli interessati o dell'obbligo di trasparenza, a meno che ciò possa compromettere la finalità di tale limitazione. Per sua natura la trasparenza impone che i titolari del trattamento forniscano anticipatamente agli interessati informazioni adeguate relative ai diritti di cui godono e alle eventuali riserve al riguardo di cui il titolare possa avvalersi, in maniera tale che l'interessato non sia colto di sorpresa dalla dichiarata limitazione di uno specifico diritto nel momento in cui successivamente tenti di esercitarlo nei confronti del titolare. Per quanto concerne la pseudonimizzazione e la minimizzazione dei dati e nella misura in cui i titolari del trattamento intendano valersi dell'articolo 11 del regolamento, il Gruppo ha precedentemente confermato nel parere 3/ 2017[56] che tale articolo dovrebbe essere interpretato come

un modo per far valere il vero principio della riduzione al minimo dei dati senza ostacolare l'esercizio dei diritti dell'interessato e che questo esercizio dev'essere reso possibile con l'ausilio delle ulteriori informazioni fornite dall'interessato.

69. L'articolo 85 impone agli Stati membri, per legge, di conciliare la protezione dei dati personali con il diritto alla libertà d'espressione e d'informazione. Ciò implica tra l'altro che, ai fini del trattamento effettuato a scopi giornalistici o di espressione accademica, artistica o letteraria, gli Stati membri prevedano, qualora siano necessarie per conciliare i due diritti, esenzioni o deroghe appropriate rispetto a determinate disposizioni del regolamento (inclusi gli obblighi di trasparenza di cui agli articoli 12-14).

TRASPARENZA E VIOLAZIONE DEI DATI

70. Il Gruppo ha elaborato linee guida distinte sulle violazioni dei dati[57], ma ai fini delle presenti linee guida gli obblighi del titolare del trattamento relativi alla comunicazione delle violazioni di dati all'interessato devono tenere integralmente conto degli obblighi di trasparenza stabiliti all'articolo 12[58]. La comunicazione di una violazione dei dati deve soddisfare gli stessi requisiti sopra illustrati (in particolare quelli sull'uso di un linguaggio semplice e chiaro), che si applicano a qualsiasi altra comunicazione con l'interessato sui suoi diritti o in connessione con la trasmissione delle informazioni di cui agli articoli 13 e 14.

ALLEGATO
INFORMAZIONI DA FORNIRE ALL'INTERESSATO
AI SENSI DELL'ARTICOLO 13 O 14

Tipo d'informazioni richieste	Articolo pertinente (se i dati personali sono raccolti direttamente presso l'interessato)	Articolo pertinente (se i dati personali non sono ottenuti presso l'interessato)	Considerazioni del Gruppo sull'obbligo d'informazione
Identità e dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante[59]	Articolo 13, paragrafo 1, lettera a)	Articolo 14, paragrafo 1, lettera a)	Le informazioni dovrebbero consentire una facile identificazione del titolare del trattamento e preferibilmente varie forme di comunicazione con esso (ad es. numero di telefono, e-mail, indirizzo postale, ecc.)
Dati di contatto del responsabile della protezione dei dati, ove applicabile	Articolo 13, paragrafo 1, lettera b)	Articolo 14, paragrafo 1, lettera b)	Si vedano le linee guida del Gruppo sui responsabili della protezione dei dati[60]
Finalità a base giuridica del trattamento	Articolo 13, paragrafo 1, lettera c)	Articolo 14, paragrafo 1, lettera c)	Oltre a definire le finalità del trattamento cui sono destinati i dati personali, dev'essere specificata la relativa base giuridica addotta ai sensi dell'articolo 6. Nel caso delle categorie particolari di dati personali si dovrebbe specificare la disposizione applicabile dell'articolo 9 (e, se del caso, il diritto

			dell'Unione o dello Stato membro applicabile al trattamento). Qualora, conformemente all'articolo 10, siano trattati dati personali relativi a condanne penali e reati oppure a correlate misure di sicurezza sulla base dell'articolo 6, paragrafo 1, si dovrebbe se del caso specificare il diritto dell'Unione o dello Stato membro applicabile al trattamento.
Legittimi interessi perseguiti dal titolare del trattamento o da un terzo qualora la base giuridica del trattamento sia costituita da legittimi interessi (articolo 6, paragrafo 1, lettera f))	Articolo 13, paragrafo 1, lettera d)	Articolo 14, paragrafo 2, lettera b)	L'interesse specifico in questione dev'essere individuato a beneficio dell'interessato. La migliore prassi prevede che il titolare del trattamento possa anche fornire all'interessato le informazioni tratte dal *test di bilanciamento*, che dev'essere svolto come base giuridica del trattamento prima di raccogliere i dati personali degli interessati per poter addurre l'articolo 6, paragrafo 1, lettera f). Per evitare un subissamento informativo, ciò può essere incluso in una dichiarazione/ informativa sulla privacy stratificata (si veda il paragrafo 35). In ogni caso, la

			posizione del Gruppo è che le informazioni fornite all'interessato debbano esplicitargli la possibilità di ottenere, su richiesta, informazioni sul test di bilanciamento. Si tratta di un aspetto essenziale per garantire una trasparenza efficace qualora l'interessato nutra dubbi circa la correttezza del test di bilanciamento o intenda proporre reclamo dinanzi a un'autorità di controllo.
Categorie di dati personali interessati	Non necessario	Articolo 14, paragrafo 1, lettera d)	Le informazioni sono richieste nell'ipotesi prevista all'articolo 14, perché i dati personali non sono stati ottenuti presso l'interessato, il quale ignora pertanto quali categorie di dati personali il titolare del trattamento abbia ottenuto.
Destinatari[61] (o categorie di destinatari) dei dati personali	Articolo 13, paragrafo 1, lettera e)	Articolo 14, paragrafo 1, lettera e)	Il termine "destinatario" è definito all'articolo 4, punto 9, come *"la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali,* ***che si tratti o meno di terzi"*** *[enfasi aggiunta].* Il destinatario non è quindi necessariamente un terzo. Gli altri titolari, contitolari

			e responsabili del trattamento ai quali sono trasferiti o comunicati i dati rientrano quindi nel concetto di "destinatario" e informazioni su di loro dovrebbero essere fornite in aggiunta alle informazioni sui destinatari terzi. Devono essere indicati i destinatari effettivi dei dati personali (per nome) o le categorie di destinatari. Conformemente al principio di correttezza, i titolari del trattamento devono fornire sui destinatari le informazioni più pregnanti per gli interessati. In pratica, si tratterà in genere dei nomi dei destinatari, in maniera tale che gli interessati sappiano con precisione chi è in possesso dei dati personali che li riguardano. Se i titolari del trattamento optano per fornire le categorie dei destinatari, le informazioni dovrebbero essere il più pecifiche possibile e indicare il tipo (ad es. facendo riferimento alle attività svolte), l'ambito di attività, il settore, il comparto e la sede dei destinatari.

Informazioni sui trasferimenti a paesi terzi, fatto stesso del trasferimento e informazioni sulle garanzie applicabili[62] (compresa la presenza o l'assenza di una decisione di adeguatezza della Commissione[63]) e strumenti per ottenerne copia o per sapere dove sono disponibili	Articolo 13, paragrafo 1, lettera f)	Articolo 14, paragrafo 1, lettera f)	Dovrebbe essere specificato l'articolo del regolamento che consente il trasferimento e il meccanismo corrispondente (ad es. decisione di adeguatezza ai sensi dell'articolo 45/norme vincolanti d'impresa ai sensi dell'articolo 47/clausole tipo di protezione dei dati ai sensi dell'articolo 46, paragrafo 2/ deroghe e garanzie ai sensi dell'articolo 49, ecc.). Dovrebbero essere fornite informazioni su dove e come accedere al documento pertinente od ottenerlo, ad es. fornendo un collegamento al meccanismo utilizzato. Conformemente al principio di correttezza, le informazioni fornite sui trasferimenti a paesi terzi dovrebbero essere il più pregnanti possibile per gli interessati. In genere, ciò significa indicare il nome dei paesi terzi.
Periodo di conservazione (o, se non disponibile, criteri per determinarlo)	Articolo 13, paragrafo 2, lettera a)	Articolo 14, paragrafo 2, lettera a)	Quest'aspetto è collegato all'obbligo di minimizzazione dei dati di cui all'articolo 5, paragrafo 1, lettera c), e a quello di limitazione della conservazione di cui all'articolo 5,

			paragrafo 1, lettera e). Il periodo di conservazione (o i criteri per determinarlo) potrebbe essere dettato da fattori quali gli obblighi di legge o le linee quida di settore, ma dovrebbe essere indicato in maniera tale da consentire all'interessato di stabilire quale sarà in base alla sua specifica situazione, il periodo previsto per i dati/fini specifici. Non è sufficiente che il titolare del trattamento affermi in maniera generica che i dati personali saranno conservati finché sarà necessario per le finalità legittime del trattamento. Ove pertinente, dovrebbero essere fissati periodi di conservazione diversi per le diverse categorie di dati personali e/o finalità del trattamento, inclusi, se del caso, i periodi di archiviazione.
Diritti dell'interessato relativamente a: • accesso • rettifica • cancellazione • limitazione del trattamento	Articolo 13, paragrafo 2, lettera b)	Articolo 14, paragrafo 2, lettera c)	Le informazioni dovrebbero essere specifiche per l'ipotesi di trattamento e comprendere una sintesi della natura dei diritti, del modo in cui l'interessato può attivarsi per esercitarli

• opposizione al trattamento • portabilità			e delle loro eventuali limitazioni (si veda il paragrafo 68). In particolare, il diritto di opporsi al trattamento dev'essere portato esplicitamente all'attenzione dell'interessato al più tardi al momento della prima comunicazione e dev'essere presentato in forma chiara e separata da qualsiasi altra informazione[64]. In relazione al diritto alla portabilità, si vedano le linee guida del Gruppo sul diritto alla portabilità dei dati[65].
Diritto di revocare il consenso in qualsiasi momento nei casi in cui il trattamento lo presuppone (in forma esplicita o altrimenti)	Articolo 13, paragrafo 2, lettera c)	Articolo 14, paragrafo 2, lettera d)	Le informazioni dovrebbero indicare il modo in cui il consenso può essere revocato, tenuto conto del fatto che esso dovrebbe poter essere revocato con la stessa facilità con cui è accordato[66].
Diritto di presentare un reclamo all'autorità di controllo	Articolo 13, paragrafo 2, lettera d)	Articolo 14, paragrafo 2, lettera e)	Le informazioni dovrebbero spiegare che, confermemente all'articolo 77, l'interessato ha diritto di presentare un reclamo all'autorità di controllo, in particolare nello Stato membro in cui risiede abitualmente o lavora oppure nel luogo ove si è verificata la presunta violazione del regolamento.

Precisazione del fatto che esista o no un obbligo previsto per legge o per contratto di fornire le informazioni o se sia necessario stipulare un contratto o se sussista l'obbligo di comunicare le informazioni, e le possibili conseguenze dell'omissione	Articolo 13, paragrafo 2, lettera e)	Non necessario	In un contesto di lavoro, ad esempio, potrebbe essere richiesto per contratto di fornire determinate informazioni al datore di lavoro presente o futuro. I moduli online dovrebbero indicare chiaramente quali campi sono "obbligatori" e quali no e quali sono le conseguenze dell'omessa compilazione dei campi obbligatori.
Fonte da cui originano i dati personali e, se applicabile, se si tratta di fonte accessibile pubblicamente	Non necessario	Articolo 14, paragrafo 2, lettera f)	Dovrebbe essere indicata la fonte specifica dei dati salvo che ciò non sia possibile; per ulteriori orientamenti si veda il paragrafo 60. Se la fonte specifica non è menzionata le informazioni fornite dovrebbero includere la natura delle fonti (ad es. pubbliche/private) e i tipi di organizzazione/ambito/settore.
Esistenza di un processo decisionale automatizzato, profilazione inclusa e, se del caso, informazioni pregnanti circa la logica seguita e l'importanza e le conseguenze previste del trattamento per gli interessati	Articolo 13, paragrafo 2, lettera f)	Articolo 14, paragrafo 2, lettera g)	Si vedano le linee guida del Gruppo su profilazione e processi decisionali automatizzati[67].

NOTE

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

[2] Le presenti linee guida stabiliscono principi generali applicabili all'esercizio dei diritti degli interessati, più che considerare modalità specifiche per ciascuno dei singoli diritti degli interessati previsti dal regolamento.

[3] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[4] Pur non essendo la trasparenza uno dei principi applicabili al trattamento dei dati personali di cui all'articolo 4 della direttiva (UE) 2016/680, il considerando 26 indica che qualsiasi trattamento di dati personali dovrebbe essere "lecito, corretto e trasparente" nei confronti della persona fisica interessata.

[5] L'articolo 1 del TUE si riferisce a decisioni prese *"nel modo più trasparente possibile e il più vicino possibile ai cittadini"*, l'articolo 11, paragrafo 2, del medesimo trattato recita: *"Le istituzioni mantengono un dialogo aperto, trasparente e regolare con le associazioni rappresentative e la società civile"* e l'articolo 15 del TFUE fa riferimento, fra l'altro, al diritto dei cittadini dell'Unione di accedere ai documenti delle istituzioni, organi e organismi dell'Unione e all'obbligo che incombe a questi di assicurare la trasparenza dei lavori svolti.

[6] "I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato".

[7] La direttiva 95/46/CE contiene solo un'allusione alla trasparenza nel considerando 38, affermando che il trattamento dei dati dovrebbe essere corretto, ma questa condizione non è richiamata espressamente nel corrispondente articolo 6, paragrafo 1, lettera a).

[8] Secondo il principio di responsabilizzazione, l'articolo 5, paragrafo 2, del regolamento obbliga il titolare del trattamento a dimostrare di aver agito in trasparenza (oltre ad aver rispettato gli altri cinque principi relativi al trattamento dei dati di cui all'articolo 5, paragrafo 1).

[9] L'articolo 24, paragrafo 1, impone al titolare del trattamento di mettere in atto misure tecniche e organizzative per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento.

[10] Si vedano ad esempio le conclusioni dell'avvocato generale Gruz Villalon (9 luglio 2015) nella causa Bara (causa C-201/14), punto 74: *"l'obbligo d'informare le persone interessate dal trattamento dei loro dati personali, a garanzia della trasparenza di qualsiasi trattamento, è ancora più rilevante poiché condiziona l'esercizio da parte loro dei diritti di accesso ai dati trattati, sancito all'articolo 12 della direttiva 95/46, e di opposizione al trattamento dei medesimi, sancito all'articolo 14 della stessa direttiva"*.

[11] Si veda il libro redatto dalla Commissione europea "Scrivere chiaro" (2011), reperibile all'indirizzo: https://publications.europa.eu/it/publication-detail/-/publication/

c2dab20c-0414-408d-87b5-dd3c6e5dd9a5.

[12] Articolo 5 della direttiva 93/13/CEE del Consiglio, del 5 aprile 1993, concernente le clausole abusive nei contratti stipulati con i consumatori.

[13] Il considerando 42 indica che è opportuno prevedere una dichiarazione di consenso predisposta da un titolare del trattamento in una forma comprensibile e facilmente accessibile, con un linguaggio semplice e chiaro e senza termini non corretti.

[14] L'obbligo di trasparenza è assolutamente indipendente da quello che incombe sui titolari del trattamento di garantire l'esistenza di una base giuridica appropriata per il trattamento, previsto all'articolo 6.

[15] Ad esempio, il fatto che il titolare del trattamento abbia un sito Internet in una data lingua e/o offra opzioni specifiche per un dato paese e/o agevoli il pagamento di beni o servizi nella valuta di un dato Stato membro può essere indicativo del fatto che si rivolge agli interessati di uno specifico Stato membro.

[16] Il termine "minore" non è definito nel regolamento. Tuttavia, il Gruppo fa presente che, in conformità della convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza, ratificata da tutti gli Stati membri dell'Unione europea, è "minore" la persona di età inferiore a 18 anni.

[17] Vale a dire i minori di almeno 16 anni di età oppure, qualora ai sensi dell'articolo 8, paragrafo 1, del regolamento il diritto nazionale dello Stato membro abbia fissato a una specifica età compresa tra 13 e 16 anni l'età a cui il minore può dare il consenso a un'offerta di fornitura di servizi della società dell'informazione, i minori che hanno l'età del consenso fissata dalla legge nazionale.

[18] Secondo il considerando 38 "[i] minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali". Il considerando 58 afferma che "[d]ato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente".

[19] https://www.unicef.it/doc/2035/pubblicazioni/i-diritti-dei-bambini-in-parole-semplici.htm.

[20] L'articolo 13 della convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza afferma: "Il fanciullo ha diritto alla libertà di espressione. Questo diritto comprende la libertà di ricercare, di ricevere e di divulgare informazioni e idee di ogni specie, indipendentemente dalle frontiere, sotto forma orale, scritta, stampata o artistica, o con ogni altro mezzo a scelta del fanciullo".

[21] Si veda la precedente nota 17.

[22] Ad esempio, la convenzione delle Nazioni Unite sui diritti delle persone con disabilità impone che a tali persone si forniscano forme appropriate di assistenza e di supporto per garantire loro l'accesso alle informazioni.

[23] L'articolo 12, paragrafo 1, fa riferimento al "linguaggio" e prevede che le informazioni siano fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici.

[24] Il Gruppo ha già riconosciuto i vantaggi delle informative stratificate nel parere 10/2004 sulla maggiore armonizzazione della fornitura d'informazioni e nel parere 02/2013 sulle applicazioni per dispositivi intelligenti.

[25] Questi esempi di mezzi elettronici hanno mera funzione indicativa e i titolari del trattamento possono sviluppare nuovi metodi innovativi per assicurare la conformità all'articolo 12.

[26] Parere 8/2014 del Gruppo, adottato il 16 settembre 2014.

[27] A norma di quest'articolo, "[l]e informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 sono gratuite".

[28] Tuttavia, conformemente all'articolo 12, paragrafo 5, il titolare del trattamento può addebitare un contributo spese ragionevole se, ad esempio, la richiesta dell'interessato relativamente alle informazioni di cui agli articoli 13 e 14 o ai diritti di cui agli articoli 15-22 o all'articolo 34 sia manifestamente infondata o eccessiva (separatamente, per quanto concerne il diritto di accesso di cui all'articolo 15, paragrafo 3, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi per ogni ulteriore copia dei dati personali richiesta dall'interessato).

[29] A titolo esemplificativo, se i dati personali dell'interessato sono raccolti in connessione con un acquisto, le informazioni da fornire ai sensi dell'articolo 13 dovrebbero essere comunicate prima del pagamento e al momento della raccolta delle informazioni, anziché a operazione conclusa. Parimenti, se sono forniti servizi gratuiti all'interessato, le informazioni di cui all'articolo 13 devono essere comunicate prima della sottoscrizione, e non dopo, dal momento che l'articolo 13, paragrafo 1, impone la fornitura delle informazioni "nel momento in cui i dati personali sono ottenuti".

[30] Conformemente ai principi di correttezza e di limitazione della finalità, l'organizzazione che raccoglie i dati personali presso l'interessato dovrebbe sempre specificare le finalità del trattamento al momento della raccolta. Se la finalità comprende la creazione di dati personali desunti da altre informazioni, la finalità prevista della creazione e dell'ulteriore trattamento di tali dati nonché le categorie dei dati desunti trattati devono essere sempre comunicate all'interessato al momento della raccolta o prima dell'ulteriore trattamento per una nuova finalità conformemente all'articolo 13, paragrafo 3, o all'articolo 14, paragrafo 4.

[31] L'espressione *"nel caso in cui i dati personali siano destinati alla …"* all'articolo 14, paragrafo 3, lettera b), contiene una specificazione della posizione generale con riferimento al limite massimo di tempo stabilito all'articolo 14, paragrafo 3, lettera a), senza però sostituirlo.

[32] L'espressione *"nel caso sia prevista la comunicazione ad altro destinatario…"* all'articolo 14, paragrafo 3, lettera c), contiene a sua volta una specificazione della posizione generale con riferimento al limite massimo di tempo stabilito all'articolo 14, paragrafo 3, lettera a), senza però sostituirlo.

[33] L'articolo 4, punto 9, definisce il termine "destinatario" e precisa che il destinatario cui sono comunicati dati personali non deve necessariamente essere un terzo. Pertanto, il destinatario può essere un titolare, un contitolare o un responsabile del trattamento.

[34] Con riferimento al principio di trasparenza il considerando 39 afferma: "Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano".

[35] Linee Guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, WP 251.

[36] Ciò vale con riferimento al processo decisionale basato unicamente su un trattamento automatizzato, profilazione inclusa, che produce effetti giuridici che riguardano l'interessato o che altrimenti incidono in modo rilevante sulla sua persona.

[37] Il considerando 60, che qui rileva, precisa che: "[i]noltre l'interessato dovrebbe essere informato dell'esistenza di una profilazione e delle conseguenze della stessa".

[38] Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento 2016/679, WP 248 rev.1.

[39] Secondo l'articolo 26, paragrafo 3, indipendentemente dalle disposizioni dell'accordo tra i contitolari del trattamento di cui al paragrafo 1 dello stesso articolo, l'interessato può esercitare i propri diritti ai sensi del regolamento nei confronti di e contro ciascun titolare del trattamento.

[40] Articolo 13, paragrafo 3, e articolo 14, paragrafo 4, formulati in modo identico a parte la parola "raccolti" usata nell'articolo 13 e sostituita da "ottenuti" nell'articolo 14.

[41] Si vedano ad esempio, su questo principio, i considerando 47, 50, 61, 156 e 158, l'articolo 6, paragrafo 4, e l'articolo 89.

[42] L'articolo 6, paragrafo 4, fissa, in modo non esaustivo, i fattori che devono essere presi in considerazione al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, ovvero: il nesso tra le finalità; il contesto in cui i dati personali sono stati raccolti; la natura dei dati personali (specialmente se sono trattate categorie particolari di dati personali oppure se sono trattati dati relativi a condanne penali e a reati); le possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; l'esistenza di garanzie adeguate.

[43] Considerando 47 e 50.

[44] Anche richiamato nel considerando 50.

[45] Come richiamato nel considerando 63, ciò consentirà all'interessato di esercitare il diritto di accesso per essere consapevole del trattamento e verificarne la liceità.

[46] "Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito web. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online".

[47] In questo contesto i titolari del trattamento dovrebbero tenere conto degli interessati con disabilità visive (ad es. affetti da daltonismo rosso-verde).

[48] Nel regolamento l'espressione "leggibile da dispositivo automatico" non è definita, ma il considerando 21 della direttiva 2013/37/UE vi si riferisce in questi termini: *"un formato di file strutturato in modo tale che le applicazioni software possano agevolmente identificarlo, riconoscerlo ed estrarne dati specifici. I dati codificati in file strutturati in un formato leggibile meccanicamente sono dati leggibili meccanicamente. I formati leggibili meccanicamente possono essere aperti o proprietari; possono essere standard formali o meno. I documenti codificati in un formato di file che limita il trattamento automatico, poiché l'estrazione dei dati in essi contenuti non è possibile o non avviene con facilità, non dovrebbero essere considerati documenti in formato leggibile meccanicamente. Gli Stati membri dovrebbero, se del caso, promuovere l'impiego di formati aperti leggibili meccanicamente"*.

[49] A norma dell'articolo 12, paragrafo 8, alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 92 al fine di stabilire le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate. Il considerando 166 (che verte sugli atti delegati della Commissione in generale) dà istruzioni in questo senso, affermando che durante i lavori preparatori la Commissione deve svolgere adeguate consultazioni, anche a livello di esperti. Tut-

tavia, il comitato europeo per la protezione dei dati detiene un importante ruolo consultivo riguardo alla standardizzazione delle icone, dal momento che l'articolo 70, paragrafo 1, lettera r), afferma che esso, di propria iniziativa o, se del caso, su richiesta della Commissione fornisce alla Commissione un parere in merito alle icone.

[50] Si veda il riferimento nel considerando 100.

[51] Secondo il capo sui diritti dell'interessato, sezione Trasparenza e modalità, del regolamento (capo III, sezione 1, nello specifico articolo 12).

[52] Accesso, rettifica, cancellazione, limitazione del trattamento, opposizione al trattamento, portabilità.

[53] Articolo 13, paragrafo 4.

[54] Articolo 25.

[55] Come stabilito agli articoli 12-22 e all'articolo 34, nonché all'articolo 5 nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli 12-22.

[56] Parere 03/2017 sul documento intitolato "Trattamento dei dati personali nel contesto del sistema di trasporto intelligente cooperativo (C-ITS)", paragrafo 4.2.

[57] Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento 2016/679, WP 250.

[58] Precisato all'articolo 12, paragrafo 1, il quale richiama specificamente il fatto di "fornire all'interessato ... le comunicazioni di cui agli articoli da 15 a 22 **e all'articolo 34** relative al trattamento...". [enfasi aggiunta].

[59] Ai sensi dell'articolo 4, punto 17, del regolamento (e come richiamato nel considerando 80), per "rappresentante" s'intende la persona fisica o giuridica stabilita nell'Unione europea che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del regolamento. L'obbligo si applica nel caso in cui, in conformità dell'articolo 3, paragrafo 2, il titolare del trattamento o il responsabile del trattamento non è stabilito nell'Unione europea, ma tratta i dati personali degli interessati che si trovano nell'Unione europea e il trattamento riguarda l'offerta di beni o la prestazione di servizi agli interessati nell'Unione europea o il monitoraggio del loro comportamento.

[60] Linee guida sui responsabili della protezione dei dati, WP243 rev. 01, versione emendata adottata il 5 aprile 2017.

[61] Quali definiti all'articolo 4, punto 9, del regolamento e richiamati nel considerando 31.

[62] Come stabilito all'articolo 46, paragrafi 2 e 3.

[63] In conformità dell'articolo 45.

[64] Articolo 21, paragrafo 4, e considerando 70 (che si applica nel caso della commercializzazione diretta).

[65] Linee guida sul diritto alla portabilità dei dati, WP 242 rev.01. Versione emendata adottata il 5 aprile 2017.

[66] Articolo 7, paragrafo 3.

[67] Linee Guida su profilazione e processi decisionali automatizzati 2016/679, WP 251.

Linee guida sul diritto alla portabilità dei dati [WP 242 rev. 01]

Adottate il 13 dicembre 2016
Versione emendata e adottata il 5 aprile 2017

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della Commissione europea, direzione generale Giustizia e consumatori, B -1049 Bruxelles, Belgio, ufficio MO59 05/35.

Sito Internet: : http://ec.europa.eu/justice/data-protection/index_en.htm

Indice

SINTESI

L'articolo 20 del regolamento generale sulla protezione dei dati introduce il nuovo diritto alla portabilità dei dati, che per molti aspetti si differenzia dal diritto di accesso pur essendo a quest'ultimo strettamente connesso. Il diritto alla portabilità dei dati permette agli interessati di ricevere i dati personali da loro forniti al titolare del trattamento, in un formato strutturato, di uso comune e leggibile meccanicamente, e di trasmetterli a un diverso titolare. L'obiettivo ultimo è accrescere il controllo degli interessati sui propri dati personali.

Consentendo la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, il diritto alla portabilità rappresenta anche uno strumento importante a supporto della libera circolazione dei dati personali nell'UE e in favore della concorrenza fra i titolari. Questo nuovo diritto faciliterà il passaggio da un fornitore di servizi all'altro e potrà, quindi, favorire la creazione di nuovi servizi nel quadro della strategia per il mercato unico digitale.

Nel parere si offrono indicazioni sull'interpretazione e sull'attuazione del diritto alla portabilità dei dati introdotto dal regolamento generale sulla protezione dei dati. L'obiettivo è analizzare questo nuovo diritto e il suo ambito di applicazione, chiarendo le condizioni di applicabilità alla luce della base legale del trattamento (consenso dell'interessato o adempimento di obblighi contrattuali) nonché nell'ottica della limitazione relativa ai dati personali forniti dall'interessato stesso. Nel parere si offrono anche esempi concreti e criteri illustrativi dei diversi contesti di applicazione. Al riguardo, il Gruppo di lavoro "Articolo 29" ritiene che il diritto alla portabilità dei dati si configu-

ri rispetto ai dati forniti consapevolmente e in modo attivo dall'interessato nonché rispetto ai dati personali generati dalle attività svolte dall'interessato. Questo nuovo diritto non può essere svuotato di contenuto limitandolo ai dati personali che sono comunicati direttamente dall'interessato, per esempio compilando un modulo online.

Sarebbe buona prassi che i titolari del trattamento iniziassero a mettere a punto gli strumenti che faciliteranno l'esercizio del diritto alla portabilità – per esempio, strumenti per il download dei dati e interfacce di programmazione di applicazioni. A loro spetta garantire che i dati personali siano trasmessi in un formato strutturato, di uso comune e leggibile meccanicamente, e li si dovrebbe invitare a garantire l'interoperabilità dei formati con cui i dati vengono messi a disposizione in ottemperanza a una richiesta di portabilità.

Il parere intende, inoltre, facilitare la comprensione da parte dei titolari del trattamento degli obblighi loro incombenti e presenta una serie di raccomandazioni relative a migliori prassi e agli strumenti che possono essere d'ausilio nell'osservanza del diritto alla portabilità dei dati. Infine, nel parere si raccomanda al mondo imprenditoriale e alle associazioni di settore di collaborare in vista della definizione di un insieme condiviso di standard e formati interoperabili che soddisfino i requisiti del diritto alla portabilità dei dati.

I. INTRODUZIONE

L'articolo 20 del regolamento generale sulla protezione dei dati (RGPD) introduce il nuovo diritto alla portabilità dei dati. Tale diritto consente all'interessato di ricevere i dati personali forniti a un titolare del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasmetterli a un altro titolare del trattamento senza impedimenti. Il diritto in questione è soggetto a determinate condizioni e mira a promuovere la libertà di scelta degli utenti, il loro controllo sui trattamenti e i loro diritti.

L'esercizio del diritto di accesso previsto dalla direttiva sulla protezione dei dati (95/46/CE) è vincolato al formato che il titolare decide di utilizzare nel fornire le informazioni richieste. **Il nuovo diritto alla portabilità intende promuovere il controllo degli interessati sui propri dati personali, facilitando la circolazione, la copia o la trasmissione dei dati da un ambiente informatico all'altro** (che si tratti dei propri sistemi, dei sistemi di soggetti terzi fidati, o di quelli di un diverso titolare del trattamento).

Il diritto in questione offre anche la possibilità di "riequilibrare" il rapporto fra interessati e titolari del trattamento tramite l'affermazione dei diritti e del controllo spettanti agli interessati in rapporto ai dati personali che li riguardano[1].

Seppure il diritto alla portabilità possa fungere da fattore di promozione della concorrenza fra i singoli servizi proprio perché facilita il passaggio da un servizio all'altro, il RGPD disciplina il trattamento dei dati personali e non la

concorrenza fra imprese. In particolare, l'articolo 20 non limita il novero dei dati portabili a quelli necessari o utili per il transito da un servizio all'altro[2].

La portabilità dei dati è un diritto nuovo; tuttavia, esistono o sono all'esame già oggi altre forme di portabilità in differenti ambiti normativi – per esempio, in rapporto alla risoluzione contrattuale, al roaming nei servizi di comunicazione, e all'accesso transfrontaliero ai servizi[3]. Potranno esservi interazioni sinergiche fra le diverse forme di portabilità se implementate in modo congiunto, seguite persino da effetti positivi per i singoli; al contempo, occorre prudenza nell'individuare possibili analogie.

Il presente parere offre indicazioni ai titolari del trattamento ai fini di un aggiornamento delle prassi, delle procedure e delle strategie adottate e chiarisce il significato della portabilità dei dati in modo da permettere agli interessati un utilizzo efficiente di questo nuovo diritto.

II. QUALI SONO LE COMPONENTI PRINCIPALI DEL DIRITTO ALLA PORTABILITÀ DEI DATI?

Il RGPD definisce il diritto alla portabilità dei dati come segue (articolo 20, paragrafo 1):

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti [...]

IL DIRITTO DI RICEVERE DATI PERSONALI

In primo luogo, la portabilità dei dati comprende il **diritto dell'interessato di ricevere un sottoinsieme dei dati personali** che lo riguardano trattati da un titolare, e di conservarli in vista di un utilizzo ulteriore per scopi personali. Tale conservazione può avvenire su un supporto personale o su un *cloud* privato, senza comportare necessariamente la trasmissione dei dati a un altro titolare del trattamento.

In questo senso, il diritto alla portabilità costituisce un'integrazione del diritto di accesso. Un aspetto specifico della portabilità consiste nel suo essere uno strumento con cui gli interessati possono facilmente gestire e riutilizzare dati personali in piena autonomia. I dati in questione devono essere ricevuti *"in un formato strutturato, di uso comune e leggibile da dispositivo automatico"*. Per esempio, un interessato potrebbe voler recuperare l'elenco dei brani musicali preferiti (o ascoltati) detenuto da un servizio di musica in streaming, per scoprire quante volte ha ascoltato determinati brani o stabilire cosa acquistare o ascoltare su un'altra piattaforma di musica digitale. Potrebbe anche voler recuperare la rubrica dei contatti di posta elettronica su web, magari per costruire una

lista degli invitati al proprio matrimonio, oppure ricavare informazioni sugli acquisti effettuati utilizzando varie carte di fidelizzazione per calcolare la propria impronta ecologica di carbonio[4].

IL DIRITTO DI TRASMETTERE DATI PERSONALI DA UN TITOLARE DEL TRATTAMENTO A UN ALTRO TITOLARE DEL TRATTAMENTO

In secondo luogo, l'articolo 20, primo paragrafo, dà agli interessati il **diritto di trasmettere dati personali da un titolare del trattamento a un altro titolare del trattamento** "senza impedimenti". I dati possono essere trasmessi direttamente da un titolare all'altro su richiesta dell'interessato, e ove ciò sia tecnicamente possibile (articolo 20, paragrafo 2). In questo senso, il considerando 68 promuove lo sviluppo di formati interoperabili da parte dei titolari così da consentire la portabilità dei dati[5], ma non configura un obbligo in capo ai titolari stessi di introdurre o mantenere sistemi di trattamento tecnicamente compatibili[6]. Tuttavia, il RGPD vieta ai titolari di creare ostacoli alla trasmissione dei dati.

In sostanza, questa componente del diritto alla portabilità configura per gli interessati la possibilità non soltanto di ottenere e riutilizzare i dati forniti a un titolare del trattamento, bensì anche di trasmettere questi dati a un diverso fornitore di servizi (appartenente allo stesso o a un diverso settore di attività). L'aspettativa è che, oltre ad ampliare il margine di controllo dei consumatori impedendo forme di "lock-in" tecnologico, il diritto alla portabilità dei dati promuova l'innovazione e la condivisione di dati personali fra titolari del trattamento in piena sicurezza e sotto il controllo dell'interessato[7]. Il diritto alla portabilità può favorire la condivisione controllata e limitata delle informazioni personali fra più soggetti e, quindi, arricchire l'esperienza dell'utente nella fruizione di determinati servizi[8]. La portabilità, inoltre, può favorire la trasmissione e il riutilizzo di dati personali fra più servizi di interesse per il singolo utente.

TITOLARITÀ DEL TRATTAMENTO

La portabilità dei dati garantisce il diritto di ricevere dati personali e di trattarli secondo la volontà dell'interessato[9].

I titolari che danno seguito a richieste di portabilità nei termini di cui all'articolo 20 non sono responsabili del trattamento effettuato dal singolo interessato o da un'altra società che riceva i dati in questione. Essi agiscono per conto dell'interessato, anche se i dati personali sono trasmessi direttamente a un diverso titolare. In questo senso, il titolare che dia seguito alla richiesta di portabilità non è responsabile dell'osservanza delle norme in materia di protezione dei dati da parte del titolare ricevente, visto che quest'ultimo non viene da lui selezionato. Al contempo, il titolare cui l'interessato si rivolge dovrebbe prevedere garanzie idonee a far sì che ogni sua attività corrisponda alle richieste

dell'interessato stesso; per esempio, potrebbe stabilire procedure atte a garantire che le categorie di dati personali trasmessi corrispondano in pieno a quelle che l'interessato desidera siano trasmesse. A tal fine, si potrebbe chiedere conferma all'interessato prima di procedere alla trasmissione, oppure in un momento antecedente quando viene prestato il consenso iniziale al trattamento ovvero viene perfezionato il contratto.

I titolari che ottemperano a una richiesta di portabilità non hanno alcun obbligo specifico di verificare la qualità dei dati prima di trasmetterli. Naturalmente i dati in questione dovrebbero già rispettare i requisiti di esattezza e aggiornamento conformemente ai principi fissati nell'articolo 5, paragrafo 1, del RGPD. Inoltre, la portabilità non impone al titolare alcun obbligo di conservazione dei dati per un periodo superiore al necessario ovvero ulteriore rispetto a quello eventualmente specificato[10]. Soprattutto, non impone alcun obbligo ulteriore di conservazione dei dati personali al solo scopo di adempiere a una potenziale richiesta di portabilità.

Qualora i dati personali oggetto della richiesta di portabilità siano trattati da un responsabile, il contratto stipulato con quest'ultimo ai sensi dell'articolo 28 del RGPD deve prevedere l'obbligo di assistere "il titolare del trattamento con misure tecniche e organizzative adeguate (...) nel dare seguito alle richieste di esercizio dei diritti dell'interessato". Pertanto, il titolare è tenuto a implementare procedure specifiche, in collaborazione con gli eventuali responsabili del trattamento, al fine di rispondere a richieste di portabilità. In presenza di contitolari del trattamento, le responsabilità attribuite a ciascun contitolare con riguardo alla gestione delle richieste di portabilità dovranno essere specificate con chiarezza in uno strumento contrattuale.

Inoltre, il titolare ricevente[11] è tenuto a garantire che i dati forniti siano pertinenti e non eccedenti rispetto al nuovo trattamento svolto. Per esempio, in caso di una richiesta di portabilità rivolta a un servizio di posta elettronica via web, se la richiesta serve all'interessato per recuperare i messaggi di posta elettronica inviandoli a una piattaforma di archiviazione, quest'ultima (il nuovo titolare) non ha necessità di trattare le informazioni di contatto dei soggetti con cui l'interessato ha scambiato messaggi. Se le informazioni non sono pertinenti rispetto alle finalità del nuovo trattamento, allora non devono essere conservate o trattate. A ogni modo, i titolari riceventi non sono tenuti ad accettare e trattare i dati personali trasmessi a seguito di una richiesta di portabilità. Analogamente, se l'interessato chiede che informazioni sulle proprie operazioni bancarie siano trasmesse a un servizio di supporto della gestione patrimoniale, il titolare ricevente non ha necessità di accettare la totalità di tali informazioni o di conservare tutti i dettagli delle operazioni in questione una volta effettuatane la categorizzazione ai fini del nuovo servizio. In altri termini, i dati accettati e conservati dovrebbero essere esclusivamente quelli necessari e pertinenti con riguardo al servizio fornito dal titolare ricevente.

Il soggetto "ricevente" assume il ruolo di titolare nei riguardi dei dati personali in questione ed è tenuto all'osservanza dei principi fissati nell'articolo 5 del

RGPD. Ne deriva che il "nuovo" titolare ricevente deve specificare con chiarezza le finalità di ogni nuovo trattamento prima che sia formulata la richiesta di trasmissione diretta dei dati portabili, conformemente con i requisiti di trasparenza fissati all'articolo 12 del regolamento[12]. Come per qualunque altra operazione di trattamento svolta sotto la sua responsabilità, il titolare dovrà applicare i principi di cui all'articolo 5 del RGPD – quali liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, integrità e riservatezza, conservazione limitata e responsabilizzazione[13].

I titolari dovrebbero predisporre quanto necessario per facilitare l'esercizio del diritto alla portabilità da parte dei rispettivi interessati. I titolari possono, inoltre, decidere se accettare dati da un interessato, ma non sono obbligati a farlo.

DIRITTO ALLA PORTABILITÀ E ALTRI DIRITTI DEGLI INTERESSATI

L'esercizio del diritto alla portabilità dei dati (o di qualsiasi altro diritto ai sensi del RGPD) non pregiudica nessuno degli altri diritti. L'interessato può continuare a fruire e beneficiare del servizio offerto dal titolare anche dopo che sia compiuta un'operazione di portabilità. La portabilità non comporta la cancellazione automatica dei dati[14] conservati nei sistemi del titolare, e non incide sul periodo di conservazione previsto originariamente per i dati oggetto di trasmissione. L'interessato può esercitare i diritti riconosciuti dal RGPD fintanto che prosegue il trattamento effettuato dal titolare.

Allo stesso modo, se l'interessato intende esercitare il diritto di cancellazione ("diritto all'oblio" ai sensi dell'articolo 17), il titolare non può procrastinare o negare tale diritto facendo valere l'esercizio del diritto alla portabilità dei dati.

Qualora l'interessato valuti che i dati personali richiesti in base al diritto alla portabilità non soddisfano che in parte le sue necessità, si dovrà dare pienamente seguito a eventuali successive richieste di dati personali formulate sulla base del diritto di accesso di cui all'articolo 15 RGPD.

Inoltre, qualora il diritto dell'UE o del singolo Stato membro preveda, con riguardo a un diverso settore, una qualche altra forma di portabilità dei dati in oggetto, nel dar seguito a una richiesta di portabilità fondata sul RGPD occorrerà tener conto anche delle condizioni fissate nelle specifiche disposizioni di settore. In primo luogo, se risulta evidente dalla richiesta presentata dall'interessato che questi intende esercitare non già i diritti previsti dal RGPD, bensì esclusivamente i diritti riconosciutigli in base alla diversa legislazione di settore, le disposizioni sulla portabilità introdotte dal RGPD non troveranno applicazione alla specifica richiesta[15]. Se, d'altro canto, la richiesta è mirata a ottenere la portabilità di cui alle disposizioni del RGPD, l'esistenza di altre norme specifiche nei termini sopra descritti non inficia in alcun modo l'applicazione generale del principio di portabilità dei dati nei riguardi del singolo titolare ai sensi del regolamento. Viceversa, occorrerà valutare caso per caso se e in che

misura tali diverse normative incidano sul diritto alla portabilità dei dati di cui al RGPD.

III. QUANDO TROVA APPLICAZIONE IL DIRITTO ALLA PORTABILITÀ DEI DATI?

A QUALI TRATTAMENTI PUÒ APPLICARSI IL DIRITTO ALLA PORTABILITÀ DEI DATI?

Per assicurare l'osservanza del RGPD, i titolari devono disporre di una base legale inoppugnabile ai fini del trattamento di dati personali.

Ai sensi dell'articolo 20, paragrafo 1, lettera a), del RGPD, **il diritto alla portabilità dei dati presuppone che il trattamento si basi:**

- **sul consenso dell'interessato** (nei termini di cui all'articolo 6, paragrafo 1, lettera a), ovvero all'articolo 9, paragrafo 2, lettera a) in caso di dati sensibili); **oppure**
- **su un contratto** di cui è parte l'interessato, nei termini di cui all'articolo 6, paragrafo 1, lettera b).

A titolo esemplificativo, i titoli dei libri acquistati da un fornitore online o la lista dei brani musicali ascoltati attraverso un servizio di streaming musicale sono, in linea di principio, dati personali che ricadono nel campo di applicazione della portabilità in quanto sono trattati per l'esecuzione di un contratto di cui è parte l'interessato.

Il regolamento non prevede un diritto generale alla portabilità dei dati il cui trattamento non si fondi sul consenso o su un contratto[16]. Per esempio, non sussiste alcun obbligo per gli istituti finanziari di ottemperare a una richiesta di portabilità relativa a dati personali che sono oggetto di trattamento nell'ambito degli obblighi di prevenzione e accertamento del reato di riciclaggio o di altri reati finanziari; allo stesso modo, il diritto alla portabilità non si applica alle informazioni di contatto di natura professionale che siano trattate nel contesto di relazioni d'impresa, se tale trattamento non si fonda sul consenso dell'interessato o su un contratto di cui quest'ultimo sia parte.

Relativamente ai dati dei dipendenti, il diritto alla portabilità trova applicazione, in via generale, solo se il trattamento si basa su un contratto di cui l'interessato (il dipendente) è parte. In molti di questi casi è difficile ipotizzare che il consenso sia prestato liberamente, a causa dello squilibrio di poteri esistente fra datore di lavoro e suoi dipendenti[17]. D'altro canto, alcuni trattamenti riferiti alla gestione delle risorse umane si fondano sull'interesse legittimo, ovvero sono necessari per adempiere a specifici obblighi di legge in materia di lavoro. In pratica, il diritto alla portabilità nel contesto della gestione del personale potrà indubbiamente trovare applicazione con riguardo a determinati trattamenti (per esempio, in rapporto alla gestione stipendi, o ai servizi di mobilità

interna), ma in molte altre situazioni occorrerà procedere caso per caso così da verificare se siano soddisfatte tutte le condizioni cui soggiace il diritto alla portabilità dei dati.

Infine, il diritto alla portabilità dei dati sussiste esclusivamente se il trattamento è "effettuato con mezzi automatizzati" e non si applica, conseguentemente, alla maggioranza degli archivi o dei registri cartacei.

QUALI DATI PERSONALI DEVONO ESSERE PORTABILI?

Ai sensi dell'articolo 20, paragrafo 1, sono portabili i dati personali che
- riguardano l'interessato, e
- sono stati *forniti* dall'interessato a un titolare.

Inoltre, l'articolo 20, paragrafo 4, stabilisce che l'osservanza del diritto alla portabilità non deve ledere i diritti e le libertà altrui.

PRIMA CONDIZIONE: DATI PERSONALI CHE RIGUARDANO L'INTERESSATO

Qualsiasi richiesta di portabilità può applicarsi solo a dati personali. Ciò significa che un dato anonimo[18] ovvero non concernente l'interessato non ricade nell'ambito di applicazione del diritto in questione. Tuttavia, un dato pseudonimo chiaramente riconducibile all'interessato (per esempio, se l'interessato stesso fornisce il rispettivo elemento di identificazione – v. articolo 11, paragrafo 2) è senza dubbio soggetto all'esercizio del diritto alla portabilità.

In molti casi i titolari trattano informazioni contenenti dati personali relativi a una pluralità di interessati; non è possibile, pertanto, dare un'interpretazione eccessivamente restrittiva dell'espressione "dati personali che riguardano l'interessato". Per esempio, i tabulati telefonici riferiti a un abbonato, la messaggistica interpersonale o i dati VoIP comprendono talora informazioni su terzi in rapporto alle chiamate in entrata e in uscita. Anche se si tratta di tabulati contenenti dati personali relativi a una pluralità di individui, l'abbonato deve avere la possibilità di ottenere tali informazioni a seguito di una richiesta di portabilità visto che i tabulati contengono (anche) dati relativi all'interessato. Se però questi stessi tabulati sono poi trasmessi a un diverso titolare del trattamento, quest'ultimo non dovrà elaborarli per finalità lesive dei diritti e delle libertà dei terzi in questione – si veda *infra*, terza condizione.

SECONDA CONDIZIONE: DATI FORNITI DALL'INTERESSATO

La seconda condizione limita l'ambito della portabilità ai dati "forniti da" un interessato.

Si possono citare numerosi esempi di dati personali che sono "forniti" consapevolmente e attivamente da un interessato, come le informazioni inserite in un modulo di registrazione online (indirizzo postale, nome utente, età, ecc.). Cionondimeno, nel novero dei dati "forniti da" un interessato rientrano anche quelli derivanti dall'osservazione delle attività svolte da tale interessato. Pertanto, il Gruppo di lavoro ritiene che, per dare pieno riconoscimento alla portata di questo nuovo diritto, la nozione di dati "forniti da" un interessato debba riferirsi anche ai dati personali osservati sulla base delle attività svolte dagli utenti, come per esempio i dati grezzi generati da un contatore intelligente o altri oggetti connessi[19], le registrazioni delle attività svolte, la cronologia della navigazione su un sito web o delle ricerche effettuate.

Non appartengono a quest'ultima categoria i dati generati dal titolare (utilizzando come input i dati osservati o forniti direttamente), per esempio il profilo-utente creato a partire dall'analisi dei dati grezzi generati da un contatore intelligente.

Si può operare una differenziazione fra le varie categorie di dati in rapporto alla rispettiva origine per stabilire se si applichi il diritto alla loro portabilità. Le categorie seguenti sono classificabili fra i dati "forniti dall'interessato":

- **dati forniti consapevolmente e attivamente dall'interessato:** indirizzo postale, nome utente, età, ecc.;
- **dati osservati forniti dall'interessato attraverso la fruizione di un servizio o l'utilizzo di un dispositivo.** Questa categoria comprende, per esempio, la cronologia delle ricerche effettuate dall'interessato, dati relativi al traffico, dati relativi all'ubicazione nonché altri dati grezzi come la frequenza cardiaca registrata da dispositivi sanitari o di fitness.

Viceversa, i dati inferenziali e derivati sono creati dal titolare sulla base dei dati "forniti dall'interessato". Per esempio, l'esito di una valutazione concernente la salute di un utente o il profilo creato nell'ambito di disposizioni in materia finanziaria e di gestione del rischio (per esempio, al fine di attribuire uno score creditizio o di ottemperare a normativa antiriciclaggio) non possono essere considerati, di per sé, dati "forniti dall'interessato". Anche se questi dati fanno parte, in certi casi, del profilo di cui è in possesso il titolare e sono dedotti o derivati dall'analisi di dati forniti dall'interessato (per esempio attraverso le attività da questi compiute), essi non sono generalmente annoverati fra i "dati forniti dall'interessato" e, pertanto, esulano dal campo di applicazione di questo nuovo diritto[20].

In linea di principio e alla luce delle finalità sottese al diritto alla portabilità dei dati, l'espressione "forniti dall'interessato" deve essere interpretata in modo estensivo escludendo unicamente "dati inferenziali" e "dati derivati", i quali comprendono i dati personali generati da un fornitore di servizi (per esempio, i risultati prodotti da un algoritmo). Il titolare può escludere i suddetti dati inferenziali e dovrebbe, invece, ricomprendervi tutti gli altri dati personali forniti dall'interessato attraverso gli strumenti messi a disposizione dal titolare stesso[21].

Pertanto, l'espressione "forniti da" si riferisce ai dati personali relativi ad attività compiute dall'interessato o derivanti dall'osservazione del comportamento di tale interessato, con esclusione dei dati derivanti dalla successiva analisi di tale comportamento. Viceversa, tutti i dati personali che siano creati dal titolare nell'ambito di un trattamento, per esempio attraverso procedure di personalizzazione o finalizzate alla formulazione di raccomandazioni, o attraverso la categorizzazione o profilazione degli utenti, sono dati derivati o dedotti dai dati personali forniti dall'interessato e non ricadono nell'ambito del diritto alla portabilità.

TERZA CONDIZIONE: IL DIRITTO ALLA PORTABILITÀ DEI DATI NON DEVE LEDERE I DIRITTI E LE LIBERTÀ ALTRUI

Per quanto riguarda i dati personali relativi ad altri interessati:
La terza condizione è intesa a evitare il recupero e la trasmissione a un nuovo titolare di informazioni contenenti i dati personali di altri interessati che a ciò non hanno acconsentito, qualora sia verosimile che tali dati siano trattati secondo modalità in grado di ledere i diritti e le libertà dei terzi interessati in questione (articolo 20, paragrafo 4, del RGPD)[22].

La lesione di cui sopra si configurerebbe, per esempio, se la trasmissione dei dati da un titolare all'altro impedisse a soggetti terzi di esercitare i diritti di cui godono in quanto interessati ai sensi del RGPD – come il diritto di informativa, accesso, ecc.

L'interessato che innesca il processo di trasmissione dei propri dati a un altro titolare presta a quest'ultimo il consenso al trattamento dei dati oppure stipula un nuovo contratto con tale titolare. Se i dati portabili contengono informazioni personali riferite a terzi, occorre individuare un diverso fondamento di liceità per il loro trattamento: per esempio, il titolare cui sono trasmessi i dati può perseguire un interesse legittimo (ai sensi dell'articolo 6, paragrafo 1, lettera f)), in particolare se il trattamento effettuato dal nuovo titolare mira alla prestazione di un servizio all'interessato per consentirgli di trattare dati personali nell'ambito di attività esclusivamente personali o familiari. I trattamenti instaurati dall'interessato nell'ambito di attività personali e che riguardino e potenzialmente incidano su soggetti terzi restano sotto la sua esclusiva responsabilità nella misura in cui non siano in alcun modo decisi dal titolare.

Per esempio, un servizio di posta elettronica via web può consentire la creazione di un registro di tutti i contatti (amici, parenti, familiari, ecc.) dell'interessato. Poiché si tratta di dati relativi a e creati da la persona fisica identificabile che desidera esercitare il proprio diritto alla portabilità, il titolare dovrebbe trasmettere all'interessato l'intero contenuto del registro con i messaggi in entrata e in uscita.

Analogamente, un conto corrente bancario può contenere dati personali relativi non soltanto alle operazioni del titolare del conto, ma anche a quelle svolte

da altri soggetti (che abbiano, per esempio, effettuato un bonifico a favore del titolare del conto). È improbabile che si configuri una lesione dei diritti e delle libertà dei terzi interessati a seguito della trasmissione al titolare del conto corrente bancario delle informazioni relative a tale conto in seguito a una richiesta di portabilità – purché nei due casi sopra citati i dati siano utilizzati per le stesse finalità, ossia come informazioni utilizzate dal solo interessato per contattare i terzi suddetti, oppure per disporre di un registro delle operazioni compiute dall'interessato sul suo conto corrente bancario.

Viceversa, i diritti e le libertà dei terzi in questione non saranno rispettati se il nuovo titolare utilizzerà i dati personali per altre finalità – per esempio, se titolare ricevente utilizza i dati personali di altri soggetti indicati nel registro dei contatti dell'interessato per finalità di marketing.

Ne deriva che, per evitare di ledere diritti e libertà dei terzi interessati, il trattamento dei dati personali in questione da parte di un diverso titolare è consentito soltanto nella misura in cui i dati rimangano nell'esclusiva disponibilità dell'utente che ne aveva richiesto la portabilità e siano utilizzati esclusivamente per finalità personali o domestiche. Il "nuovo" titolare che ha ricevuto tali dati (anche direttamente, se così chiede l'utente) non può utilizzare i dati riferiti a terzi per le proprie finalità – per esempio, per proporre offerte di marketing e servizi ai suddetti terzi, o per arricchire il profilo dei terzi interessati e ricostruire il loro contesto sociale a loro insaputa e senza il loro consenso[23]. Né può utilizzarli per ricavare informazioni sui terzi in oggetto e creare profili specifici, anche se già ne detiene i dati personali. In caso contrario, è verosimile che il trattamento risulti illecito e violi il principio di correttezza, soprattutto se i terzi in questione non ricevono informativa e non sono in grado di esercitare i diritti loro riconosciuti in quanto interessati dal trattamento.

Inoltre, per ridurre ulteriormente i rischi a carico di altri interessati i cui dati siano passibili di portabilità, è opportuno che tutti i titolari – sia coloro che "inviano" sia coloro che "ricevono" i dati – rendano disponibili strumenti per consentire agli interessati di scegliere i dati che desiderano trasmettere e ricevere escludendo (se del caso) i dati di altri interessati.

Sarebbe anche opportuna l'implementazione da parte dei titolari di meccanismi per la prestazione del consenso da parte di altri interessati coinvolti nell'esercizio della portabilità, in modo da facilitare la trasmissione dei loro dati qualora anch'essi siano favorevoli – per esempio, se anch'essi intendono trasferire i propri dati a un diverso titolare del trattamento. Un caso del genere potrebbe ben presentarsi con le reti di socializzazione *(social networks)*, ma spetta ai titolari decidere quale buona prassi implementare.

Per quanto riguarda dati soggetti a diritti di proprietà intellettuale o informazioni commerciali riservate:
I diritti e le libertà altrui sono menzionati all'articolo 20, paragrafo 4. Pur se non direttamente connesso alla portabilità, si può ritenere che ciò comprenda anche *"il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i*

diritti d'autore che tutelano il software". Tuttavia, benché sia opportuno tenere conto dei diritti in questione prima di rispondere a una richiesta di portabilità, *"tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni"*. Inoltre, il titolare non dovrebbe respingere una richiesta di portabilità a motivo della violazione di un altro diritto contrattuale – per esempio, a causa dell'esistenza di morosità o di un contenzioso commerciale con l'interessato.

Il diritto alla portabilità dei dati non comporta il diritto di abusare dei dati fino a configurare prassi scorrette ovvero in violazione dei diritti di proprietà intellettuale.

Tuttavia, l'esistenza di un rischio potenziale per l'attività imprenditoriale non può, isolatamente e in quanto tale, costituire fondamento per il diniego della richiesta di portabilità: i titolari possono trasmettere i dati personali forniti dagli interessati in un formato tale da non rivelare informazioni commerciali riservate o soggette a diritti di proprietà intellettuale.

IV. COME TROVANO APPLICAZIONE RISPETTO ALLA PORTABILITÀ DEI DATI LE NORME GENERALI CHE DISCIPLINANO L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI?

QUALI INFORMAZIONI DEVONO ESSERE FORNITE PREVENTIVAMENTE AGLI INTERESSATI?

Per rispettare il nuovo diritto alla portabilità dei dati, i titolari devono informare gli interessati dell'esistenza di tale diritto. Qualora i dati personali in questione siano raccolti direttamente presso l'interessato, l'informativa deve essere fornita "nel momento in cui i dati personali sono ottenuti". Se, invece, i dati personali non sono stati ottenuti direttamente dall'interessato, il titolare deve fornire l'informativa nei termini previsti dagli artt. 13, paragrafo 2, lettera b) [sic], e 14, paragrafo 2, lettera c) del RGPD.

"Qualora i dati personali non siano stati ottenuti presso l'interessato", l'articolo 14, paragrafo 3, prevede che l'informativa sia fornita entro un termine ragionevole e comunque non superiore a un mese dall'ottenimento dei dati, in occasione della prima comunicazione con l'interessato ovvero al momento della comunicazione dei dati a terzi[24].

Nel fornire le informazioni necessarie, i titolari devono aver cura di distinguere il diritto alla portabilità da altri diritti. In particolare, il Gruppo di lavoro "Articolo 29" raccomanda ai titolari di spiegare con chiarezza la differenza fra le categorie di dati che un interessato può ricevere attraverso l'esercizio del diritto alla portabilità anziché del diritto di accesso.

Inoltre, il Gruppo di lavoro raccomanda ai titolari di informare sempre dell'esistenza del diritto alla portabilità prima che gli interessati procedano alla chiu-

sura di un account. In tal modo gli utenti potranno avere contezza dei propri dati personali e trasmetterli con facilità a un proprio dispositivo ovvero a un altro fornitore di servizi prima della rescissione del contratto.

Infine, il Gruppo di lavoro raccomanda ai titolari "riceventi" di fornire agli interessati un'informativa completa sulla natura dei dati personali pertinenti ai fini della prestazione del rispettivo servizio. Oltre a costituire il fondamento della correttezza del trattamento, ciò permetterà agli utenti di ridurre i rischi per i terzi interessati e di evitare inutili duplicazioni di dati personali anche ove non siano coinvolti altri interessati.

COME FA IL TITOLARE A IDENTIFICARE L'INTERESSATO PRIMA DI RISPONDERE A UNA SUA RICHIESTA?

Il RGPD non contiene prescrizioni specifiche rispetto all'eventuale autenticazione di un interessato. Cionondimeno, l'articolo 12, paragrafo 2, del regolamento stabilisce che il titolare non può rifiutarsi di dar seguito alla richiesta di esercizio dei diritti avanzata da un interessato (compreso il diritto alla portabilità dei dati), salvo che il trattamento di dati personali persegua uno scopo che non rende necessaria l'identificazione dell'interessato e il titolare possa dimostrare di non essere in grado di identificare l'interessato. Tuttavia, in casi del genere l'interessato stesso può fornire informazioni ulteriori ai fini della propria identificazione da parte del titolare – come prevede l'articolo 11, paragrafo 6. L'articolo 12, paragrafo 2, stabilisce, inoltre, che qualora il titolare nutra ragionevoli dubbi circa l'identità dell'interessato, può chiedere informazioni ulteriori per confermarne l'identità. Se l'interessato fornisce effettivamente tali informazioni ulteriori che ne consentono l'identificazione, il titolare non può rifiutarsi di dar seguito alla richiesta. Se dati e/o informazioni raccolti online sono collegati a pseudonimi o identificativi unici, i titolari possono istituire idonee procedure così da permettere all'interessato di presentare una richiesta di portabilità ottenendo i dati che lo riguardano. In ogni caso, i titolari devono prevedere una procedura di autenticazione in modo da stabilire con certezza l'identità dell'interessato che chiede i propri dati personali o, più in generale, chiede di esercitare i diritti riconosciutigli dal RGPD.

In molti casi procedure del tipo sopra descritto sono già in essere. Spesso gli interessati devono superare una fase di autenticazione prima di stipulare un contratto con il titolare o di prestare il consenso al trattamento. Ne deriva che i dati personali utilizzati per la registrazione dell'interessato possono essere utilizzati anche ai fini dell'autenticazione di tale interessato in rapporto all'esercizio della portabilità[25].

In casi del genere la necessità di identificare preventivamente l'interessato può imporre la richiesta di una prova giuridicamente valida della sua identità; tuttavia, non sempre occorre una verifica di questo tipo al fine di stabilire una connessione fra i dati e la persona cui i dati si riferiscono, poiché tale connessione non ha niente a che fare con l'identità ufficiale o giuridicamente provata

della persona in questione. In sostanza, la possibilità riconosciuta al titolare di chiedere informazioni ulteriori per accertare l'identità dell'interessato non può comportare richieste eccedenti né la raccolta di dati personali che non sono pertinenti né necessari al fine di rafforzare il legame fra interessato e dati personali oggetto della richiesta.

In molti casi procedure di autenticazione del tipo sopra descritto sono già in essere. Per esempio, spesso si utilizza un nome utente e una password per consentire all'utente di accedere ai propri dati negli account di posta elettronica, sulle piattaforme social, o in molti altri servizi – che in certi casi gli utenti scelgono di utilizzare senza rivelare il nome per esteso e la propria identità.

Se il volume dei dati richiesti dall'interessato rende problematica la trasmissione via Internet, il titolare potrebbe valutare il ricorso a modalità alternative invece di fare affidamento sull'estensione potenziale del periodo previsto per la risposta all'interessato (massimo tre mesi)[26]. Per esempio, potrebbe ricorrere allo streaming, oppure salvare i dati su CD, DVD o altri supporti fisici, oppure ancora consentire la trasmissione diretta dei dati personali a un diverso titolare (come prevede l'articolo 20, paragrafo 2, del regolamento, se tecnicamente possibile).

QUAL È LA TEMPISTICA PER OTTEMPERARE A UNA RICHIESTA DI PORTABILITÀ?

In base all'articolo 12, paragrafo 3, il titolare fornisce *"informazioni relative all'azione intrapresa"* all'interessato *"senza ingiustificato ritardo"* e comunque "entro un mese dal ricevimento dalla richiesta" ovvero, in casi di particolare complessità, entro un massimo di tre mesi, purché l'interessato venga informato delle motivazioni di tale proroga entro un mese dal ricevimento della richiesta iniziale.

I titolari che gestiscono servizi della società dell'informazione dispongono probabilmente di migliori strumenti per ottemperare a queste richieste in tempi estremamente ridotti. Per venire incontro alle aspettative degli utenti, è buona prassi indicare la tempistica normalmente applicabile alla gestione delle richieste di portabilità informandone gli interessati.

I titolari che oppongono un diniego alla richiesta di portabilità devono indicare all'interessato, ai sensi dell'articolo 12, paragrafo 4, *"[de]i motivi dell'inottemperanza e [del]la possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale"* al più tardi entro un mese dal ricevimento della richiesta.

I titolari devono rispettare l'obbligo di ottemperare nei termini previsti, anche in caso di diniego. In altri termini, l'inattività non è ammessa qualora un titolare riceva una richiesta di portabilità.

IN QUALI CASI È POSSIBILE OPPORRE DINIEGO A UNA RICHIESTA DI PORTABILITÀ O ADDEBITARE UN CONTRIBUTO PER OTTEMPERARVI?

L'articolo 12 vieta al titolare di addebitare oneri all'interessato per la fornitura dei dati personali, salvo dimostrare il carattere manifestamente infondato o eccessivo delle richieste *"in particolare per il loro carattere ripetitivo"*. Nel caso di servizi della società dell'informazione specializzati nel trattamento automatizzato di dati personali, il ricorso a sistemi automatizzati quali le interfacce di programmazione di applicazioni (API, *Application Programming Interfaces*)[27] può facilitare le interazioni con l'interessato e, quindi, ridurre gli oneri potenzialmente derivanti da richieste aventi carattere ripetitivo. Dovrebbero dunque essere molto rari i casi in cui il titolare potrà giustificare il diniego delle informazioni richieste, anche in caso di richieste multiple.

Inoltre, per determinare se una richiesta sia eccessiva, non è corretto tenere conto dei costi complessivamente generati dalle procedure introdotte per rispondere a richieste di portabilità. In realtà, l'articolo 12 del regolamento guarda alle richieste presentate da un singolo interessato, e non già al numero complessivo di richieste ricevute dal singolo titolare. Ne consegue che i costi legati all'implementazione del sistema di risposta a richieste di questo tipo non devono essere imputati agli interessati né assunti a giustificazione del diniego di una richiesta di portabilità.

V. IN CHE MODO DEVONO ESSERE MESSI A DISPOSIZIONE I DATI PORTABILI?

QUALI SONO GLI STRUMENTI CHE IL TITOLARE DOVREBBE PREDISPORRE AL FINE DI FORNIRE I DATI RICHIESTI?

L'articolo 20, paragrafo 2, del RGPD prevede che gli interessati hanno il diritto di trasmettere i dati a un diverso titolare senza impedimenti da parte del titolare cui li hanno forniti.

Gli impedimenti in questione possono consistere in ostacoli di natura giuridica, tecnica o finanziaria con cui il titolare evita o rallenta l'accesso, la trasmissione o il riutilizzo da parte dell'interessato o di un diverso titolare. Per esempio, potrebbe trattarsi della richiesta di un corrispettivo per fornire i dati richiesti, dell'indisponibilità di formati interoperabili o dell'accesso a un'API o al formato in cui i dati vengono forniti, dell'eccessiva complessità insita nel recupero della totalità dei dati richiesti o dell'eccessiva lunghezza del periodo necessario a tale scopo, dell'offuscamento deliberato dei dati in oggetto, o di vincoli settoriali specifici e ingiustificati o eccessivi in termini di standard o accreditamenti richiesti[28].

Inoltre, l'articolo 20, paragrafo 2, obbliga il titolare a trasmettere i dati portabili direttamente a un diverso titolare "se tecnicamente fattibile".

La fattibilità tecnica della trasmissione da un titolare all'altro, sotto il controllo dell'interessato, deve essere valutata caso per caso. Il considerando 68 chiarisce i limiti di ciò che è "tecnicamente fattibile", specificando che "non dovrebbe comportare l'obbligo per i titolari di adottare o mantenere sistemi di trattamento tecnicamente compatibili".

L'aspettativa è che il titolare trasmetta i dati personali in un formato interoperabile, ma ciò non configura alcun obbligo in capo agli altri titolari di supportare tale formato. Pertanto, la trasmissione diretta dei dati da un titolare all'altro potrebbe avvenire se è possibile instaurare una comunicazione fra due sistemi, in modo sicuro[29], e se il sistema ricevente è tecnicamente in grado di ricevere i dati in ingresso. Qualora impedimenti di ordine tecnico precludano la trasmissione diretta, il titolare deve illustrarne l'esistenza agli interessati poiché, in caso contrario, la sua decisione sarà nei fatti analoga a un diniego di intervento nei confronti della richiesta formulata dall'interessato (articolo 12, paragrafo 4).

Sul piano tecnico, i titolari dovrebbero esplorare e valutare due approcci diversi e complementari per mettere a disposizione degli interessati o di altri titolari dati che siano portabili:

- trasmissione diretta dell'intero insieme di dati portabili (o di più estratti di parti del set complessivo di dati);
- utilizzo di uno strumento automatizzato che consenta l'estrazione dei dati pertinenti.

Il secondo approccio sarà forse preferibile per quei titolari che hanno a che fare con insiemi complessi e di grandi dimensioni, in quanto permette di estrarre quelle parti del set di dati che sono pertinenti per l'interessato nel contesto della sua specifica richiesta, può favorire la minimizzazione del rischio, e probabilmente consente il ricorso a meccanismi di sincronizzazione dei dati[30] – per esempio, nel contesto di comunicazioni regolari fra titolari del trattamento. Si tratta di un approccio forse più idoneo a garantire l'osservanza delle norme da parte del "nuovo" titolare, e potrebbe configurare una buona prassi per ridurre i rischi in termini di privacy da parte del titolare iniziale.

Nell'implementare i due approcci diversi e complementari sopra indicati, al fine di fornire i dati portabili volta per volta pertinenti, si possono prevedere varie metodologie: l'utilizzo di messaggistica sicura, di un server SFTP, di una WebAPI o di un WebPortal sicuri. Al fine di conservare i dati personali e consentire ai singoli titolari di accedervi e trattarli nei modi necessari, gli interessati dovrebbero avere la possibilità di utilizzare un *personal data store*, ossia un servizio di deposito per i propri dati personali, un sistema per la gestione delle informazioni personali[31] ovvero altri meccanismi basati sulla presenza di "terzi fidati" *(trusted third parties)*.

QUAL È IL FORMATO PREVISTO PER I DATI?

Il RGPD pone in capo ai titolari del trattamento l'obbligo di fornire i dati personali richiesti dall'interessato in un formato che ne consenta il riutilizzo. Più in particolare, l'articolo 20, paragrafo 1, del regolamento stabilisce che i dati personali devono essere forniti "*in un formato strutturato, di uso comune e leggibile da dispositivo automatico*". Nel considerando 68 si chiarisce ulteriormente che il formato in questione dovrebbe essere interoperabile, termine la cui definizione[32] nell'UE è la seguente:

> *la capacità di organizzazioni diverse e disparate di interagire in vista di obiettivi comuni concordati e reciprocamente vantaggiosi, ricorrendo alla condivisione di conoscenze e informazioni tra le organizzazioni, per mezzo dei processi aziendali che su di esse si basano, tramite lo scambio di dati fra i rispettivi sistemi TIC.*

I termini "strutturato", "di uso comune" e "leggibile da dispositivo automatico" costituiscono requisiti minimi che intendono facilitare l'interoperabilità del formato dei dati messi a disposizione dal titolare. In tal senso, si tratta di specificazioni dello strumento da utilizzare, mentre l'interoperabilità è l'obiettivo finale.

Nel considerando 21 della direttiva 2013/37/UE[33,34] si rinviene la seguente definizione dell'espressione "leggibile meccanicamente" [machine readable nel testo inglese]:

> *un formato di file strutturato in modo tale che le applicazioni software possano agevolmente identificarlo, riconoscerlo ed estrarne dati specifici. I dati codificati in file strutturati in un formato leggibile meccanicamente sono dati leggibili meccanicamente. I formati leggibili meccanicamente possono essere aperti o proprietari; possono essere standard formali o meno. I documenti codificati in un formato di file che limita il trattamento automatico, poiché l'estrazione dei dati in essi contenuti non è possibile o non avviene con facilità, non dovrebbero essere considerati documenti in formato leggibile meccanicamente. Gli Stati membri dovrebbero, se del caso, promuovere l'impiego di formati aperti leggibili meccanicamente.*

Considerato l'ampio ventaglio di tipologie di dati potenzialmente oggetto di trattamento da parte di un titolare, il RGPD non contiene indicazioni specifiche sul formato dei dati personali da fornire agli interessati. I formati più idonei saranno diversi in rapporto ai singoli settori di attività e verosimilmente già oggi esistono formati adeguati; la scelta del formato dovrebbe essere sempre orientata all'obiettivo ultimo di consentire l'interpretabilità e di offrire all'interessato un ampio margine di portabilità. In tal senso, non si potrebbe ritenere adeguato l'impiego di un formato soggetto a costosi vincoli di licenza.

Nel considerando 68 si chiarisce che *"Il diritto dell'interessato di trasmettere o ricevere dati personali che lo riguardano non dovrebbe comportare l'obbligo per i titolari del trattamento di adottare o mantenere sistemi di trattamento tecnicamente*

compatibili". **Ciò significa che la portabilità intende produrre sistemi interoperabili, non sistemi compatibili**[35].

I dati personali dovrebbero essere messi a disposizione in un formato con un livello elevato di astrazione rispetto a qualsiasi formato a uso interno o proprietario. In sostanza, la portabilità dei dati comporta un ulteriore livello di trattamento da parte dei titolari, al fine di estrarre i dati dalla piattaforma filtrando le informazioni personali che non ricadono nell'ambito della portabilità quali i dati dedotti o quelli connessi alla sicurezza di un sistema. In tal modo, i titolari sono spinti a individuare in precedenza, a monte, i dati che, nei rispettivi sistemi, ricadono nell'ambito del diritto alla portabilità. Questo trattamento aggiuntivo sarà da ritenersi accessorio rispetto al trattamento principale, poiché non è effettuato per conseguire una ulteriore finalità definita dal titolare.

Qualora non vi siano formati di impiego comune in un determinato settore di attività o in un determinato contesto, **i titolari dovrebbero fornire i dati personali utilizzando formati aperti di impiego comune (per esempio: XML, JSON, CSV, ecc.) unitamente a metadati utili, al miglior livello possibile di granularità**, mantenendo un livello elevato di astrazione. In tal senso, si dovrebbero utilizzare idonei metadati così da descrivere con precisione il significato delle informazioni oggetto di transazione. I metadati dovrebbero essere sufficienti a consentire la funzionalità e il riutilizzo dei dati, ovviamente senza rivelare segreti industriali. Pertanto, fornire all'interessato la versione in formato pdf delle informazioni contenute nella sua casella di "posta elettronica in arrivo" sarebbe poco conciliabile con il requisito di un formato sufficientemente strutturato o descrittivo, tale da permettere con facilità il riutilizzo dei dati contenuti nella casella di posta. I dati relativi alla posta elettronica dovrebbero essere messi a disposizione dell'utente in un formato che garantisca l'integrità di tutti i metadati in modo da consentirne l'effettivo ed efficace riutilizzo. In tal senso, nella scelta del formato, il titolare dovrebbe valutare in che modo tale formato ostacoli o incida sul diritto dell'interessato al riutilizzo dei dati forniti. Se il titolare è in grado di offrire più opzioni all'interessato quanto al formato preferito per i dati personali portabili, dovrebbe essere prevista anche un'informativa perspicua sugli effetti prodotti dalle singole opzioni. D'altro canto, non è possibile fondare legittimamente il trattamento di ulteriori metadati esclusivamente sul presupposto di una loro necessità o utilità ai fini dell'adempimento di un'eventuale richiesta di portabilità.

Il Gruppo di lavoro sostiene con forza la ricerca di forme di collaborazione fra i produttori e le associazioni di categoria al fine di sviluppare un insieme condiviso di standard e formati interoperabili che soddisfino i requisiti del diritto alla portabilità dei dati. Questa sfida è stata raccolta anche dallo *European Interoperability Framework* (EIF), che ha elaborato un approccio condiviso all'interoperabilità pensato per i soggetti che intendano prestare servizi pubblici in modo congiunto. Limitatamente al suo ambito di applicazione, questo schema specifica una serie di elementi comuni comprendenti un

lessico condiviso, concetti, principi, politiche, linee-guida, raccomandazioni, standard, specifiche e prassi[36].

COME GESTIRE INSIEMI ESTESI O COMPLESSI DI DATI PERSONALI?

Il RGPD non spiega come gestire la risposta a richieste di portabilità in presenza di insiemi estesi o strutturalmente complessi di dati né quando si presentino altre problematiche tecniche che comportino potenziali difficoltà per i titolari o gli interessati.

Resta comunque essenziale che il singolo abbia la possibilità di comprendere appieno l'ambito concettuale e la struttura di fondo dei dati personali che il titolare sarebbe in grado di mettere a sua disposizione. Per esempio, si potrebbe prevedere che i dati siano forniti in prima istanza in forma sintetica, attraverso appositi "pannelli" *(dashboards)* che permettano quindi all'interessato di applicare la portabilità a sottoinsiemi dei dati personali anziché alla loro totalità. Il titolare dovrebbe fornire un quadro d'insieme *"in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro"* (si veda l'articolo 12, paragrafo 1, del regolamento) così che l'interessato sappia sempre con chiarezza quali dati scaricare o trasmettere a un diverso titolare in rapporto a una specifica finalità. Per esempio, l'interessato dovrebbe essere in grado di utilizzare applicazioni software per individuare, riconoscere e trattare con facilità specifici segmenti di informazione.

Come sopra ricordato, un possibile approccio alla gestione delle richieste di portabilità consiste nel mettere a disposizione degli interessati una API adeguatamente sicura e documentata. In tal modo i singoli interessati avrebbero la possibilità di chiedere al titolare la portabilità dei propri dati personali attraverso programmi sviluppati in proprio o da terzi, ovvero di consentire ad altri (anche a un diverso titolare) di presentare tali richieste per loro conto come previsto dall'articolo 20, paragrafo 2, del regolamento. Utilizzando API accessibili dall'esterno per consentire l'accesso ai dati sarebbe forse possibile prevedere anche un sistema di accesso maggiormente sofisticato, che consenta ai singoli di presentare richieste successive effettuando un download completo dei dati ovvero soltanto delle modifiche intervenute dopo l'ultimo download – senza che tali richieste ulteriori comportino oneri per il titolare.

COME GARANTIRE LA SICUREZZA DEI DATI PORTABILI?

In via generale, il titolare deve garantire la "adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali" – come previsto dall'articolo 5, paragrafo 1, lettera f), del RGPD.

Tuttavia, anche la trasmissione di dati personali all'interessato può comportare problematiche in termini di sicurezza.

COME FA IL TITOLARE A GARANTIRE CHE I DATI PERSONALI SIANO FORNITI IN MODO SICURO AL DESTINATARIO CORRETTO?

Considerato che la portabilità mira a trasportare dati personali all'esterno del sistema informativo del titolare, la fase di trasmissione può essere fonte di rischio per i dati portabili – soprattutto in termini di violazioni dei dati che possono verificarsi durante la loro trasmissione. Il titolare ha la responsabilità dell'adozione di tutte le misure di sicurezza necessarie a garantire non soltanto la trasmissione sicura dei dati personali (attraverso la crittografia end-to-end) al destinatario corretto (attraverso misure di autenticazione "forte"), ma anche la permanente tutela dei dati personali che rimangono nel suo sistema, nonché procedure trasparenti per la gestione di eventuali violazioni dei dati[37]. In tal senso, i titolari dovrebbero valutare i rischi specificamente legati alla portabilità dei dati e adottare idonee misure di mitigazione del rischio.

Le misure suddette potrebbero comprendere quanto segue: se è già necessario procedere all'autenticazione dell'interessato, il ricorso a ulteriori informazioni di autenticazione (per esempio, un segreto condiviso) o a un ulteriore fattore di autenticazione (per esempio, una password monouso); se vi sono motivi per sospettare una compromissione dell'*account*, la sospensione o il congelamento della trasmissione; in caso di trasmissione diretta da un titolare all'altro, si dovrebbe ricorrere a meccanismi di autenticazione delegata, per esempio l'autenticazione tramite *token*.

Tali misure di sicurezza non devono avere natura ostruttiva e non devono ostacolare l'esercizio dei diritti da parte degli utenti (per esempio, a causa di costi ulteriori).

COME AIUTARE GLI UTENTI A CONSERVARE I DATI PERSONALI NEI PROPRI SISTEMI IN MODO SICURO?

Una volta recuperati i propri dati personali da un sistema online, esiste sempre il rischio che gli utenti li conservino in sistemi meno sicuri di quello di partenza. L'interessato che chiede di ricevere informazioni ha la responsabilità di individuare le misure corrette al fine di garantire la sicurezza dei dati personali nel proprio sistema. Tuttavia, dovrebbe essere sensibilizzato al riguardo in modo da adoperarsi per tutelare le informazioni ricevute. Quale prassi consigliata, il titolare potrebbe anche raccomandare l'impiego di idonei formati, strumenti di crittografia e altre misure di sicurezza al fine di facilitare l'interessato in questa impresa.

* * *

Fatto a Bruxelles il 13 dicembre 2016

Per il Gruppo di lavoro,
La Presidente
Isabelle FALQUE-PIERROTIN

Versione emendata e adottata in data
5 aprile 2017

Per il Gruppo di lavoro
La Presidente
Isabelle FALQUE-PIERROTIN

NOTE

[1] L'obiettivo primario del diritto alla portabilità è potenziare il controllo dei singoli sui dati personali che li riguardano assicurando agli interessati un ruolo attivo nell'ecosistema delle informazioni.

[2] Per esempio, il diritto alla portabilità può consentire alle banche di fornire servizi aggiuntivi, sotto il controllo dell'utente, attraverso l'impiego di dati personali raccolti inizialmente nel quadro della fornitura di servizi energetici.

[3] Si veda l'agenda della Commissione europea per il mercato unico digitale: https://ec.europa.eu/digital-agenda/en/digital-single-market, in particolare il primo pilastro della relativa strategia denominato "Migliorare l'accesso online ai beni e ai servizi digitali".

[4] In questi casi il trattamento effettuato dall'interessato può ricadere nell'ambito delle attività per fini personali o familiari – se rimane interamente soggetto al controllo del solo interessato – oppure può essere svolto da un soggetto terzo per conto dell'interessato. In quest'ultima evenienza il soggetto terzo deve essere considerato un autonomo titolare del trattamento anche al solo fine della conservazione dei dati, e dovrà quindi rispettare i principi e gli obblighi previsti nel RGPD.

[5] Si veda anche la sezione V.

[6] Pertanto, occorrerà prestare particolare attenzione al formato dei dati trasmessi in modo da garantire che i dati siano riutilizzabili dall'interessato o da un diverso titolare con un minimo sforzo. Si veda anche la sezione V.

[7] Si vedano varie applicazioni sperimentali in Europa, per esempio MiData nel Regno Unito o MesInfos/SelfData di FING in Francia.

[8] I benefici (e i rischi) legati alla combinazione di dati personali provenienti dai diversi ambiti di attività di una persona emergono con evidenza in rapporto alla cosiddetta "quantificazione del sé" e all'Internet delle Cose – si pensi all'associazione di informazioni sulla forma fisica, le attività svolte e l'apporto calorico per delineare un quadro più organico, riunito in un singolo file, delle abitudini di vita di un interessato.

[9] Il diritto alla portabilità non si limita ai dati personali utili e pertinenti ai fini della prestazione di servizi analoghi da parte di soggetti concorrenti del titolare.

[10] Nell'esempio sopra riportato, se un titolare non conserva traccia dei brani musicali riprodotti da un utente, questi dati personali non potranno essere inclusi fra i dati portabili a seguito della relativa richiesta.

[11] Cioè il titolare che riceve dati personali a seguito di una richiesta di portabilità presentata dall'interessato a un altro titolare.

[12] Inoltre, il nuovo titolare dovrebbe astenersi dal trattare dati personali che non siano pertinenti, e il trattamento dovrebbe limitarsi ai dati necessari per le nuove finalità anche se i dati personali in questione fanno parte di un più ampio insieme di dati trasmessi attraverso una procedura di portabilità. I dati personali che non risultano necessari per le finalità perseguite dal nuovo trattamento devono essere cancellati quanto prima.

[13] Una volta ricevuti dal titolare, i dati personali trasmessi nell'ambito dell'esercizio del diritto alla portabilità possono essere considerati dati "forniti" dall'interessato e possono, quindi, essere ritrasmessi in base a tale diritto, nella misura in cui siano soddisfatte le altre

condizioni applicabili (base legale del trattamento, ...).

[14] Si veda l'articolo 17 del RGPD.

[15] Per esempio, se la richiesta presentata dall'interessato mira specificamente a permettere a un fornitore di servizi di informazione sui conti di accedere ai movimenti sul proprio conto corrente bancario, per le finalità di cui alla direttiva 2 sui servizi di pagamento (PSD2), tale accesso dovrebbe essere consentito in base alle disposizioni della suddetta direttiva.

[16] Si vedano il considerando 68 e l'articolo 20, paragrafo 3, del RGPD. Questi ultimi stabiliscono che la portabilità non sussiste qualora il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, ovvero qualora il titolare agisca nell'esercizio di funzioni pubbliche o per l'adempimento di un obbligo legale. Ne deriva che un titolare non è tenuto a prevedere procedure di portabilità in casi del genere. Tuttavia, è buona prassi mettere a punto meccanismi che consentano di rispondere in modo automatico a richieste di portabilità alla luce dei principi che disciplinano tale diritto. Per esempio, si pensi a un servizio di matrice governativa che consenta di scaricare con facilità le dichiarazioni dei redditi pregresse. Sulla portabilità quale buona prassi in caso di trattamenti fondati sul presupposto della necessità al fine di tutelare un interesse legittimo, e sulle procedure istituite in tal senso su base volontaria, si vedano le pagine 47 e 48 del parere 6/2014 del Gruppo di lavoro sull'interesse legittimo (WP217).

[17] Si veda, sul punto, il parere 8/2001 del Gruppo di lavoro del 13 settembre 2001 (WP48).

[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_it.pdf.

[19] Potendo ottenere i dati derivanti dall'osservazione delle sue attività, l'interessato disporrà anche di un quadro più completo delle modalità implementative seguite dal titolare quanto all'ambito dei dati osservati e potrà scegliere con cognizione di causa quali dati fornire per ottenere un servizio analogo, oltre ad apprezzare in quale misura sia rispettato il suo diritto alla privacy.

[20] Ciononostante, l'interessato può sempre esercitare il "diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali" nonché informazioni riguardanti "l'esistenza di decisioni automatizzate, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato", in base all'articolo 15 del RGPD (relativo al diritto di accesso).

[21] Ivi compresi tutti i dati osservati con riguardo all'interessato nel corso delle attività per le cui finalità i dati sono raccolti – per esempio, l'anagrafica delle operazioni svolte o i log di accesso. Anche i dati raccolti attraverso il tracciamento e la registrazione dell'interessato (come nel caso di un'app che registri la frequenza cardiaca o dei dispositivi utilizzati per tracciare le abitudini di navigazione) dovrebbero essere annoverati fra quelli "forniti" dall'interessato benché non siano trasmessi in modo attivo o consapevole.

[22] In base al considerando 68 del RGPD, "[q]ualora un certo insieme di dati personali riguardi più di un interessato, il diritto di ricevere i dati personali non dovrebbe pregiudicare i diritti e le libertà degli altri interessati in ottemperanza del presente regolamento".

[23] Un social network non dovrebbe arricchire il profilo degli iscritti utilizzando dati personali trasmessi da un interessato nell'esercizio del di-

ritto alla portabilità, senza rispettare il principio di trasparenza e verificare di disporre di un'idonea base legale con riguardo a tale specifico trattamento.

[24] L'articolo 12 prevede che i titolari forniscano "le comunicazioni [...] in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori".

[25] Per esempio, se il trattamento è effettuato in rapporto a un account utente, fornire il nome utente e la password utilizzati a tale scopo può bastare per identificare l'interessato.

[26] V. articolo 12, paragrafo 3.

[27] Per API, o interfacce di programmazione di applicazioni, si intendono interfacce di applicazioni o servizi web che i titolari rendono disponibili per consentire ad altri sistemi o applicazioni di connettersi e operare con i propri sistemi.

[28] Alcuni ostacoli possono insorgere legittimamente, per esempio in quanto connessi ai diritti e alle libertà altrui di cui all'articolo 20, paragrafo 4, ovvero alla sicurezza dei sistemi del titolare. Spetta al titolare giustificare la legittimità di tali ostacoli e il fatto che non si tratti di impedimenti ai sensi dell'articolo 20, paragrafo 1.

[29] Tramite comunicazione autenticata con il livello necessario di cifratura.

[30] I meccanismi di sincronizzazione possono favorire il rispetto degli obblighi generali fissati nell'articolo 5 del RGPD, in base al quale i "dati personali sono (...) esatti e, se necessario, aggiornati".

[31] Per quanto riguarda i sistemi per la gestione di informazioni personali (PIMS), si veda, per esempio, il parere 9/2016 del GEPD, disponibile qui: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf.

[32] Articolo 2 della decisione n. 922/2009/CE del Parlamento europeo e del Consiglio, del 16 settembre 2009, relativa a soluzioni interoperabili per le amministrazioni pubbliche europee (ISA) (GU L 260 del 3.10.2009, pag. 20).

[33] Recante modifiche della direttiva 2003/98/CE sul riutilizzo dell'informazione del settore pubblico.

[34] Il glossario UE (http://eur-lex.europa.eu/eli-register/glossary.html) fornisce ulteriori indicazioni sulle aspettative connesse alle nozioni cui si fa riferimento nelle presenti linee-guida, quali "leggibile meccanicamente", "interoperabilità", "formato aperto", "standard" e "metadato".

[35] Lo standard ISO/IEC 2382-01 definisce l'interoperabilità come segue: "La capacità di comunicare, eseguire programmi o trasferire dati fra diverse unità funzionali in una modalità che richiede all'utente conoscenze minime o nulle delle caratteristiche peculiari di tali unità".

[36] Fonte: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf.

[37] Conformemente alla direttiva (UE) 2016/1148 relativa a misure per un livello elevato comune di sicurezza delle reti e dei sistemi informativi nell'Unione.

WP242 Allegato - Domande frequenti

1. Qual è l'obiettivo del diritto alla portabilità dei dati?

La portabilità dei dati sostanzialmente permette agli interessati di ottenere e riutilizzare i "propri" dati per i propri scopi e attraverso servizi diversi. In questo senso, facilita la circolazione, la copia o il trasferimento dei dati personali da un ambiente informatico all'altro senza impedimenti. Oltre ad ampliare il margine di controllo dei consumatori impedendo forme di "lock-in" tecnologico, si prevede che il diritto alla portabilità dei dati promuoverà l'innovazione e la condivisione di dati personali fra titolari del trattamento in piena sicurezza e sotto il controllo dell'interessato.

2. Cosa è possibile ottenere esercitando il diritto alla portabilità?

In primo luogo, si ha il diritto di ricevere dati personali ("in un formato strutturato, di uso comune e leggibile meccanicamente") trattati da un titolare del trattamento e di memorizzarli su un dispositivo nella propria disponibilità in vista di un successivo utilizzo personale, senza trasferirli a un diverso titolare. Si tratta, dunque, di un diritto che facilita la gestione diretta dei propri dati personali.

In secondo luogo, si ha il diritto di trasmettere i propri dati personali da un titolare del trattamento a un altro "senza impedimenti". Si tratta, dunque, di un diritto che facilita per gli interessati la circolazione, la copia o il trasferimento di dati personali da un ambiente informatico all'altro.

3. A quali strumenti è consigliabile ricorrere per dare seguito a richieste di portabilità?

I titolari del trattamento dovrebbero, in primo luogo, offrire agli interessati la possibilità di effettuare direttamente il download delle informazioni; in secondo luogo, dovrebbero consentire agli interessati la trasmissione diretta di queste informazioni a un diverso titolare – per esempio, mettendo a disposizione degli interessati un'interfaccia di programmazione di applicazioni.

Gli interessati potrebbero anche voler ricorrere a servizi di deposito e memorizzazione dei dati personali o a un terzo fiduciario, in modo da conservare i dati mettendoli a disposizione di singoli titolari di trattamento in base a quanto necessario così da semplificare il trasferimento dei dati da un titolare all'altro.

4. In che misura un titolare del trattamento ha la responsabilità dei dati trasferiti o ricevuti a seguito dell'esercizio del diritto alla portabilità?

I titolari del trattamento che danno seguito a richieste di portabilità non sono responsabili del trattamento effettuato dal singolo interessato o da un'altra so-

cietà che riceve i dati in questione. D'altra parte, il titolare del trattamento che riceve i dati è tenuto a garantire che i dati a lui forniti siano pertinenti e non eccedenti rispetto al nuovo trattamento svolto, che l'interessato sia stato informato con chiarezza delle finalità di tale nuovo trattamento e, più in generale, che siano rispettati tutti i principi in materia così come fissati dal regolamento.

5. L'esercizio del diritto alla portabilità dei dati produce effetti sull'esercizio degli altri diritti di cui gode l'interessato?

L'esercizio del diritto alla portabilità dei dati (e di ogni altro diritto ai sensi del regolamento) lascia impregiudicati tutti gli altri diritti. L'interessato può esercitare i propri diritti fintanto che il titolare tratta i dati. Per esempio, l'interessato può continuare a usufruire del servizio offerto dal titolare anche dopo aver esercitato il diritto alla portabilità dei dati. Allo stesso modo, se intende chiedere la cancellazione dei dati, opporsi al trattamento o accedere ai propri dati personali, l'esercizio pregresso o successivo del diritto alla portabilità non è utilizzabile dal titolare quale giustificazione di un rifiuto o del ritardo nel dare seguito a tali richieste. La portabilità non comporta la cancellazione automatica dei dati conservati nei sistemi del titolare, e non incide sul periodo di conservazione previsto originariamente per i dati oggetto di trasmissione a seguito dell'esercizio del diritto alla portabilità.

6. Quando trova applicazione il diritto alla portabilità dei dati?

Affinché questo nuovo diritto possa applicarsi occorre che siano soddisfatte **tutte e tre le condizioni** indicate di seguito.

In primo luogo, i dati personali devono essere trattati, attraverso strumenti automatizzati (quindi escludendo gli archivi cartacei), sulla base del consenso preventivo dell'interessato o per l'esecuzione di un contratto di cui è parte l'interessato.

In secondo luogo, i dati personali di cui si chiede la portabilità devono riguardare l'interessato ed essere quelli forniti dall'interessato. Il Gruppo di lavoro raccomanda ai titolari del trattamento di non interpretare l'espressione "dati personali che riguardano l'interessato" in modo eccessivamente restrittivo, qualora vi siano dati personali di terzi all'interno di un insieme di dati che riguardano l'interessato e sono stati forniti da quest'ultimo, e che l'interessato utilizza per scopi personali. Ne sono un esempio, tipicamente, i tabulati telefonici, che contengono le chiamate in entrata e quelle in uscita, oppure il prospetto dei movimenti sul proprio conto corrente bancario, in cui sono riportati anche gli accrediti effettuati da soggetti terzi.

Si può ritenere che un dato personale sia fornito dall'interessato se quest'ultimo lo "fornisce" consapevolmente e in modo attivo: è il caso, per esempio, dei dati di registrazione (indirizzo postale, nome utente, età, ecc.) inseriti compilando un modulo online. Tuttavia, la definizione comprende anche i dati generati e raccolti attraverso le attività dell'utente che fruisce di un servizio o

utilizza un dispositivo. Viceversa, il diritto alla portabilità non si applica ai dati personali che sono derivati o dedotti dalle informazioni fornite dall'interessato (per esempio, il profilo-utente creato analizzando i dati grezzi di un contatore intelligente), poiché non si tratta di dati forniti dall'interessato bensì creati dal titolare del trattamento.

In terzo luogo, l'esercizio del diritto alla portabilità non deve ledere i diritti e le libertà altrui. Per esempio, se l'insieme dei dati trasferiti su richiesta dell'interessato contiene dati personali che riguardano altre persone fisiche, il nuovo titolare dovrebbe trattare tali dati solo in presenza di un'idonea base giuridica. È questo il caso di un trattamento che sia svolto direttamente dall'interessato nell'ambito di attività esclusivamente personali o domestiche.

7. Come informare gli interessati di questo nuovo diritto?

I titolari del trattamento devono informare gli interessati dell'esistenza del diritto alla portabilità "in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro". A questo proposito, il Gruppo di lavoro raccomanda ai titolari di illustrare con chiarezza la differenza fra le categorie di dati che un interessato può ricevere esercitando il diritto alla portabilità anziché il diritto di accesso, e di informare gli interessati specificamente in merito all'esistenza del diritto alla portabilità prima di chiudere un account, così da permettere loro di recuperare e conservare i propri dati personali.

Inoltre, i titolari che ricevono dati portabili su richiesta dell'interessato possono, quale migliore prassi, fornire agli interessati un'informativa completa sulla natura dei dati personali pertinenti ai fini della prestazione del rispettivo servizio.

8. Come fa il titolare del trattamento a identificare l'interessato prima di rispondere a una sua richiesta?

Il Gruppo di lavoro raccomanda ai titolari del trattamento di mettere in atto procedure idonee a consentire agli interessati di presentare una richiesta di portabilità e di ricevere i dati personali che li riguardano. I titolari devono prevedere una procedura di autenticazione in modo da stabilire con certezza l'identità dell'interessato che chiede i propri dati personali o, più in generale, chiede di esercitare i diritti riconosciutigli dal regolamento generale sulla protezione dei dati.

9. Qual è la tempistica per rispondere a una richiesta di portabilità?

L'articolo 12 vieta al titolare del trattamento di addebitare oneri all'interessato per la fornitura dei dati personali, salvo dimostrare il carattere manifestamente infondato o eccessivo delle richieste "in particolare per il loro carattere ripetitivo". In via generale, appare molto improbabile che il fatto di dover rispondere a richieste plurime di portabilità comporti un onere eccessivo per un

fornitore di servizi della società dell'informazione o di analoghi servizi online, specializzato nei trattamenti automatizzati di dati personali. In casi del genere, il Gruppo di lavoro raccomanda di definire una tempistica ragionevole che tenga conto dello specifico contesto, informandone gli interessati.

10. In che modo devono essere messi a disposizione i dati portabili?

I dati personali devono essere trasmessi in un formato strutturato, di uso comune e leggibile meccanicamente. Queste specifiche, relative alla modalità di trasmissione, intendono garantire l'interoperabilità dei formati messi a disposizione dai titolari, che rappresenta l'obiettivo ultimo. Tuttavia, ciò non significa che i titolari debbano dotarsi di sistemi compatibili. Inoltre, i titolari dovrebbero fornire, unitamente ai dati, quanti più metadati possibile al miglior livello possibile di granularità, così da preservare la semantica specifica delle informazioni oggetto di scambio.

Tenuto conto della molteplicità di categorie di dati potenzialmente oggetto di trattamento, il regolamento generale sulla protezione dei dati non contiene indicazioni specifiche per i titolari quanto al formato dei dati personali da fornire agli interessati. La scelta del formato più idoneo dipenderà dallo specifico settore di attività e probabilmente esistono già oggi formati adeguati allo scopo; in ogni caso, la scelta dello specifico formato deve essere ispirata all'obiettivo ultimo dell'interoperabilità.

Il Gruppo di lavoro sostiene con forza la ricerca di forme di collaborazione fra i produttori e le associazioni di categoria al fine di sviluppare un insieme condiviso di standard e formati interoperabili che soddisfino i requisiti del diritto alla portabilità dei dati.

Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 [WP 251 rev. 01]

Adottate il 3 ottobre 2017
Versione emendata e adottata in data 6 febbraio 2018

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 della stessa,

visto il suo regolamento interno,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della Commissione europea, direzione generale Giustizia e consumatori, B-1049 Bruxelles, Belgio, ufficio MO-59 05/35.

Sito internet: http://ec.europa.eu/justice/data-protection/index_en.htm

Indice

I. INTRODUZIONE

Il regolamento generale sulla protezione dei dati tratta in maniera specifica la profilazione e il processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione[1].

La profilazione e il processo decisionale automatizzato sono utilizzati in un numero crescente di settori, tanto privati quanto pubblici. Banche e finanza, assistenza sanitaria, fiscalità, assicurazioni, marketing e pubblicità sono soltanto alcuni esempi dei settori nei quali la profilazione viene effettuata con maggiore regolarità a sostegno del processo decisionale.

I progressi tecnologici e le capacità in materia di analisi dei megadati (big data), intelligenza artificiale e apprendimento automatico hanno reso più facile la creazione di profili e l'adozione di decisioni automatizzate, con potenziali ripercussioni significative sui diritti e sulle libertà delle persone fisiche.

La diffusa disponibilità di dati personali su Internet e di quelli ricavabili dai dispositivi di Internet delle cose, associata alla capacità di trovare correlazioni

e creare collegamenti, può consentire la determinazione, l'analisi e la previsione di aspetti della personalità, del comportamento, degli interessi e delle abitudini di una persona.

La profilazione e il processo decisionale automatizzato possono essere utili per le persone fisiche e le organizzazioni, offrendo loro vantaggi quali:

- miglioramenti dell'efficienza;
- risparmi di risorse.

Presentano inoltre numerose applicazioni commerciali: ad esempio, possono essere utilizzati per segmentare meglio i mercati e personalizzare i servizi e i prodotti allineandoli alle singole esigenze. Anche la medicina, l'istruzione, l'assistenza sanitaria e i trasporti possono beneficiare di questi processi.

Tuttavia, la profilazione e il processo decisionale automatizzato possono comportare rischi significativi per i diritti e le libertà delle persone fisiche, che richiedono garanzie adeguate.

Questi processi possono essere poco trasparenti. Le persone fisiche potrebbero non sapere di essere profilate o non comprenderne le conseguenze.

La profilazione può perpetuare stereotipi e la segregazione sociale. Può anche confinare una persona in una categoria specifica e limitarla alle preferenze suggerite per tale categoria. Ciò può minare la libertà delle persone di scegliere, ad esempio, determinati prodotti o servizi quali libri, musica o newsfeed. In taluni casi, la profilazione può portare a previsioni imprecise, in altri al diniego di servizi e beni e a discriminazioni ingiustificate.

Il regolamento introduce nuove disposizioni per far fronte ai rischi derivanti dalla profilazione e dal processo decisionale automatizzato, in particolare, ma non solo, in relazione alla tutela della vita privata. Le presenti linee guida mirano a chiarire tali disposizioni.

Il presente documento tratta i seguenti temi:

- definizioni di profilazione e processo decisionale automatizzato e approccio del regolamento a tali aspetti in generale – capitolo II
- disposizioni generali sulla profilazione; e sul processo decisionale automatizzato – capitolo III;
- disposizioni specifiche sulle decisioni basate unicamente sul trattamento automatizzato di cui all'articolo 22 - capitolo IV
- minori e profilazione – capitolo; V
- valutazioni d'impatto sulla protezione; dei dati e responsabili della protezione dei dati – capitolo VI.

Gli allegati contengono alcune raccomandazioni sulle migliori prassi, basate sull'esperienza accumulata negli Stati membri.

Il Gruppo di lavoro articolo 29 per la protezione dei dati (Gruppo di lavoro) monitorerà l'attuazione delle presenti linee guida e provvederà alle integrazioni che si riveleranno opportune.

II. DEFINIZIONI

Il regolamento introduce disposizioni per garantire che la profilazione e il processo decisionale automatizzato relativo alle persone fisiche (comprensivo o meno di profilazione) non siano utilizzati in maniera tale da avere un impatto ingiustificato sui diritti delle persone. Esso prevede ad esempio:

- requisiti specifici di trasparenza e correttezza;
- maggiori obblighi in termini di responsabilizzazione;
- basi giuridiche specifiche per il trattamento;
- il diritto delle persone fisiche di opporsi alla profilazione, segnatamente alla profilazione per finalità di marketing;
- qualora siano soddisfatte determinate condizioni, la necessità di effettuare una valutazione d'impatto sulla protezione dei dati.

Il regolamento non si concentra soltanto sulle decisioni prese a seguito di un trattamento automatizzato o della profilazione. Si applica anche alla raccolta di dati per la creazione di profili e all'applicazione di tali profili alle persone fisiche.

A. PROFILAZIONE

Il regolamento definisce la profilazione all'articolo 4, punto 4, come:

> qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

La profilazione è costituita da tre elementi:

- deve essere una forma di trattamento *automatizzato*;
- deve essere effettuata su *dati personali*;
- il suo obiettivo deve essere quello di *valutare aspetti personali* relativi a una persona fisica.

L'articolo 4, punto 4, fa riferimento a "qualsiasi forma di trattamento automatizzato" e non al trattamento "unicamente" automatizzato (di cui all'articolo 22). La profilazione deve implicare una qualche forma di trattamento automa-

tizzato, sebbene il coinvolgimento umano non comporti necessariamente l'esclusione dell'attività dalla definizione.

La profilazione è una procedura che può implicare una serie di deduzioni statistiche. Spesso viene impiegata per effettuare previsioni su persone usando dati provenienti da varie fonti per dedurre qualcosa su una persona in base alle qualità di altre persone che sembrano statisticamente simili.

Il regolamento afferma che la profilazione è il trattamento automatizzato di dati personali per valutare determinati aspetti personali, in particolare per analizzare o prevedere aspetti riguardanti persone fisiche. L'uso del verbo "valutare" suggerisce che la profilazione implichi una qualche forma di valutazione o giudizio in merito a una persona.

La semplice classificazione di persone basata su caratteristiche note quali età, sesso e altezza non determina necessariamente una profilazione. Quest'ultima dipende infatti dalla finalità della classificazione.

Ad esempio, un'azienda potrebbe voler classificare i propri clienti in base all'età o al sesso per finalità statistiche e per acquisire una panoramica aggregata dei propri clienti senza effettuare previsioni o trarre conclusioni in merito a una persona specifica. In questo caso, la finalità non è la valutazione delle caratteristiche individuali e quindi non si tratta di profilazione.

Il regolamento si ispira alla definizione di profilazione di cui alla raccomandazione CM/Rec (2010)13[2] del Consiglio d'Europa ma non la riprende tale e quale, infatti la raccomandazione esclude il trattamento che non include la deduzione. Tuttavia, la raccomandazione spiega in maniera utile che la profilazione può comportare tre fasi distinte:

- raccolta dei dati;
- analisi automatizzata per individuare correlazioni;
- applicazione della correlazione a una persona fisica per individuare caratteristiche di comportamento presenti o future.

Il titolare del trattamento che effettua la profilazione dovrà assicurarsi di soddisfare le prescrizioni del regolamento in relazione a tutte le fasi di cui sopra.

In generale, la profilazione consiste nella raccolta di informazioni su una persona (o un gruppo di persone) e nella valutazione delle loro caratteristiche o dei loro modelli di comportamento al fine di includerli in una determinata categoria o gruppo, in particolare per analizzare e/o fare previsioni, ad esempio, in merito a:

- capacità di eseguire un compito;
- interessi, o
- comportamento probabile.

Esempio

Un intermediario di dati raccoglie dati da diverse fonti pubbliche e private, per conto dei suoi clienti o per finalità proprie. Raccoglie i dati per sviluppare profili sulle persone e inserirle in segmenti e poi vende queste informazioni alle imprese che desiderano migliorare l'orientamento dei loro beni e servizi. L'intermediario di dati esegue la profilazione inserendo una persona in una determinata categoria in base ai suoi interessi.

L'esistenza o meno di un processo decisionale automatizzato, così come definito nell'articolo 22, paragrafo 1, dipenderà dalle circostanze.

B. PROCESSO DECISIONALE AUTOMATIZZATO

Il processo decisionale automatizzato ha una portata diversa da quella della profilazione, a cui può sovrapporsi parzialmente o da cui può derivare. Il processo decisionale esclusivamente automatizzato consiste nella capacità di prendere decisioni impiegando mezzi tecnologici senza coinvolgimento umano. Le decisioni automatizzate possono essere basate su qualsiasi tipo di dati, ad esempio:

- dati forniti direttamente dall'interessato (come le risposte a un questionario);
- dati osservati riguardo a una persona (come i dati relativi all'ubicazione raccolti tramite un'applicazione);
- dati derivati o desunti, come un profilo della persona che è già stato creato (ad esempio un punteggio sull'affidabilità creditizia).

Le decisioni automatizzate possono essere prese ricorrendo o meno alla profilazione, la quale a sua volta può essere svolta senza che vengano prese decisioni automatizzate. Tuttavia, la profilazione e il processo decisionale automatizzato non sono necessariamente attività separate. Qualcosa che inizia come un semplice processo decisionale automatizzato potrebbe diventare un processo basato sulla profilazione, a seconda delle modalità di utilizzo dei dati.

Esempio

Infliggere una multa per eccesso di velocità esclusivamente sulla base delle prove fornite dall'autovelox è un processo decisionale automatizzato che non implica necessariamente la profilazione.

Tuttavia la decisione di infliggere la multa sarebbe basata sulla profilazione se le abitudini di guida della persona in questione fossero state monitorate nel tempo e, ad esempio, l'ammontare della multa fosse il risultato di una valutazione che coinvolge altri fattori quali l'eventuale recidiva di eccesso di velocità o l'eventuale recente violazione di altre disposizioni del codice della strada.

Le decisioni che non sono unicamente automatizzate potrebbero includere anche la profilazione. Ad esempio, prima di concedere un mutuo, un istituto bancario può prendere in considerazione il punteggio sull'affidabilità creditizia del mutuatario, associandolo a ulteriori interventi significativi svolti da esseri umani prima che venga adottata qualsiasi decisione relativa alla persona in questione.

C. APPROCCIO DEL REGOLAMENTO A QUESTI CONCETTI

Esistono potenzialmente tre modalità d'uso della profilazione:

I) profilazione generale;
II) processo decisionale basato sulla profilazione;
III) decisione basata *unicamente* sul trattamento automatizzato, compresa la profilazione, che produce effetti giuridici o incide in modo analogo significativamente sull'interessato (articolo 22, paragrafo 1).

La differenza tra i punti ii) e iii) è dimostrata più chiaramente dai due esempi che seguono, nei quali una persona chiede un prestito online:

- un essere umano decide se accordare il prestito sulla base di un profilo prodotto con mezzi unicamente automatizzati - punto ii);
- un algoritmo decide se il prestito viene accordato e la decisione viene trasmessa automaticamente alla persona, senza alcuna previa valutazione significativa da parte di un essere umano - punto iii).

Il titolare del trattamento può svolgere attività di profilazione e processi decisionali automatizzati purché sia in grado di soddisfare tutti i principi e disponga di una base legittima per il trattamento. Garanzie supplementari e limitazioni si applicano nel caso di decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, di cui all'articolo 22, paragrafo 1.

Il capitolo III delle presenti linee guida spiega le disposizioni del regolamento per *tutti* i processi decisionali automatizzati relativi alle persone fisiche e di profilazione. Ciò include i processi decisionali che *non* sono unicamente automatizzati.

Il capitolo IV delle presenti linee guida spiega le disposizioni specifiche che si applicano *esclusivamente* al processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione[3]. Esiste un divieto generale relativamente a questo tipo di trattamento al fine di riflettere i potenziali rischi per i diritti e le libertà delle persone fisiche.

III. DISPOSIZIONI GENERALI SULLA PROFILAZIONE E SUL PROCESSO DECISIONALE AUTOMATIZZATO

La presente panoramica delle disposizioni si applica a tutte le profilazioni e a tutti i processi decisionali automatizzati. Qualora il trattamento soddisfi la

definizione di cui all'articolo 22, paragrafo 1, si applicano le disposizioni specifiche supplementari di cui al capitolo IV.

A. PRINCIPI IN MATERIA DI PROTEZIONE DEI DATI

I principi in materia di protezione dei dati sono pertinenti per tutte le attività di profilazione e tutti i processi decisionali automatizzati che comportano l'uso di dati personali[4]. Al fine di agevolare il rispetto delle norme, il titolare del trattamento dovrebbe considerare i seguenti elementi fondamentali:

1. ARTICOLO 5, PARAGRAFO 1, LETTERA A) - LICEITÀ, CORRETTEZZA E TRASPARENZA

La trasparenza del trattamento[5] è una prescrizione fondamentale sancita dal regolamento.

Spesso il processo di profilazione è invisibile all'interessato. Funziona creando dati derivati o desunti in merito a persone fisiche, ossia dati personali "nuovi" che non sono stati forniti direttamente dagli interessati. Le persone fisiche hanno gradi diversi di comprensione e per alcune potrebbe essere difficile comprendere le complesse tecniche coinvolte nella profilazione e nei processi decisionali automatizzati.

Ai sensi dell'articolo 12, paragrafo 1, il titolare del trattamento deve fornire agli interessati informazioni concise, trasparenti, intelligibili e facilmente accessibili sul trattamento dei loro dati personali[6].

Per i dati raccolti direttamente dall'interessato, tali informazioni devono essere fornite al momento della raccolta (articolo 13); per i dati ottenuti indirettamente, le informazioni devono essere fornite entro i termini stabiliti all'articolo 14, paragrafo 3.

Esempio

Alcuni assicuratori offrono tariffe e servizi assicurativi in base al comportamento di guida delle persone. Gli elementi presi in considerazione in questi casi potrebbero includere la distanza percorsa, il tempo trascorso alla guida e l'itinerario percorso, nonché previsioni basate su altri dati raccolti dai sensori dell'auto (intelligente). I dati raccolti vengono utilizzati per fini di profilazione con l'obiettivo di individuare comportamenti di guida errati (come accelerazione rapida, frenata improvvisa ed eccesso di velocità). Queste informazioni possono essere incrociate con altre fonti (ad esempio il clima, il traffico, il tipo di strada) in maniera da comprendere meglio il comportamento del conducente.

Il titolare del trattamento deve assicurarsi di disporre di una base legittima per tale tipo di trattamento. Il titolare del trattamento deve inoltre fornire all'interessato informazioni sui dati raccolti e, se del caso, sull'esistenza di processi decisionali automatizzati di cui all'articolo 22, paragrafi 1 e 4, sulla logica applicata, nonché sulla rilevanza e sulle conseguenze previste di tale trattamento.

I requisiti specifici riguardanti le informazioni e l'accesso ai dati personali sono esaminati nei capitoli III (sezione D) e IV (sezione E).

Il trattamento deve inoltre essere corretto e trasparente.

La profilazione può essere iniqua e creare discriminazioni, ad esempio negando l'accesso a opportunità di lavoro, credito o assicurazione oppure offrendo prodotti finanziari eccessivamente rischiosi o costosi. L'esempio seguente, che non rispetta le prescrizioni di cui all'articolo 5, paragrafo 1, lettera a), illustra come una profilazione iniqua può portare a proporre ad alcuni consumatori offerte meno interessanti rispetto ad altri.

Esempio

Un intermediario di dati vende profili di consumatori a società finanziarie senza il consenso dei consumatori o senza che essi conoscano i dati sottostanti. I profili classificano i consumatori in categorie (con diciture quali "popolazione rurale e che ce la fa a malapena", "membro di una minoranza etnica che vive in povertà in una realtà urbana secondaria", "inizi difficili: giovani genitori single") oppure assegnano loro dei punteggi, concentrandosi sulla vulnerabilità finanziaria dei consumatori. Le società finanziarie offrono a questi consumatori prestiti a breve termine (payday loan) e altri servizi finanziari "non tradizionali" (prestiti a costo elevato e altri prodotti finanziariamente rischiosi)[7].

2. ARTICOLO 5, PARAGRAFO 1, LETTERA B) - ULTERIORE TRATTAMENTO E LIMITAZIONE DELLA FINALITÀ

La profilazione può comportare l'utilizzo di dati personali originariamente raccolti per una finalità diversa.

Esempio

Alcune applicazioni mobili forniscono servizi di localizzazione che consentono all'utente di trovare ristoranti nelle vicinanze che offrono sconti. Tuttavia, i dati raccolti vengono utilizzati anche per creare un profilo dell'interessato per finalità di marketing, ossia per individuare le sue preferenze alimentari o il suo stile di vita in generale. L'interessato si aspetta che i suoi dati vengano utilizzati per trovare ristoranti, ma non per ricevere pubblicità relative alla consegna di pizza a domicilio soltanto perché l'applicazione ha stabilito che arriva a casa tardi. Questo ulteriore utilizzo dei dati relativi all'ubicazione potrebbe non essere compatibile con le finalità per le quali tali dati sono stati originariamente raccolti e può quindi richiedere il consenso dell'interessato[8].

La compatibilità di tale ulteriore trattamento con le finalità originarie per le quali i dati sono stati raccolti dipenderà da una serie di fattori[9], tra gli altri, le informazioni che il titolare del trattamento ha inizialmente fornito all'interessato. Tali fattori si riflettono nel regolamento[10] e sono così riassunti:

- il rapporto tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento;
- il contesto in cui i dati personali sono stati raccolti e le ragionevoli aspettative dell'interessato in merito al loro uso futuro;
- la natura dei dati;
- l'impatto dell'ulteriore trattamento sull'interessato;
- le garanzie applicate dal titolare del trattamento per assicurare un trattamento corretto e prevenire qualsiasi impatto indebito sull'interessato.

3. ARTICOLO 5, PARAGRAFO 1, LETTERA C) - MINIMIZZAZIONE DEI DATI

Le opportunità commerciali create dalla profilazione, da costi di memorizzazione più economici e dalla capacità di trattare grandi quantità di informazioni possono incoraggiare le organizzazioni a raccogliere più dati personali di quelli di cui hanno effettivamente bisogno, poiché tali dati potrebbero rivelarsi utili in futuro. Il titolare del trattamento deve assicurarsi di rispettare il principio di minimizzazione dei dati e le prescrizioni dei principi di limitazione della finalità e limitazione della conservazione.

Il titolare del trattamento dovrebbe essere in grado di spiegare in maniera chiara e giustificare la necessità della raccolta e della conservazione dei dati personali oppure prendere in considerazione l'utilizzo di dati aggregati, anonimizzati o (laddove ciò consenta una protezione sufficiente) pseudonimizzati per la profilazione.

4. ARTICOLO 5, PARAGRAFO 1, LETTERA D) - ESATTEZZA

Il titolare del trattamento dovrebbe esaminare l'esattezza in tutte le fasi del processo di profilazione, in particolare quando:

- raccoglie i dati;
- analizza i dati;
- crea un profilo per una persona o
- applica un profilo per prendere una decisione su una persona.

Se i dati utilizzati nel contesto di un processo decisionale automatizzato o di profilazione non sono esatti, qualsiasi decisione o profilo che ne deriverà sarà viziato. Le decisioni possono essere prese sulla base di dati obsoleti o di un'interpretazione errata di dati esterni. Eventuali inesattezze possono portare a previsioni o affermazioni inappropriate in merito, ad esempio, alla salute, al rischio di credito o al rischio assicurativo di una data persona.

Anche qualora i dati grezzi siano registrati in maniera esatta, l'insieme dei dati potrebbe non essere pienamente rappresentativo oppure l'analisi potrebbe contenere distorsioni nascoste.

Il titolare del trattamento deve introdurre misure efficaci per verificare e assicurare su base continuativa che i dati riutilizzati od ottenuti indirettamente siano esatti e aggiornati. Ciò sottolinea ulteriormente l'importanza di fornire informazioni chiare sui dati personali trattati, in maniera da consentire all'interessato di correggere eventuali inesattezze e migliorare la qualità dei dati.

5. ARTICOLO 5, PARAGRAFO 1, LETTERA E) - LIMITAZIONE DELLA CONSERVAZIONE

Gli algoritmi di apprendimento automatico sono progettati per trattare grandi volumi di informazioni e creare correlazioni che consentano alle organizzazioni di creare profili estremamente esaustivi e personali delle persone fisiche. Sebbene possano esservi vantaggi nel conservare i dati in caso di profilazione, dal momento che sarà disponibile una quantità maggiore di dati dai quali l'algoritmo può apprendere, il titolare del trattamento deve rispettare il principio di minimizzazione dei dati all'atto della raccolta e assicurare che i dati non siano conservati per un periodo superiore a quello necessario e proporzionato alle finalità per le quali i dati vengono trattati.

La politica di conservazione del titolare del trattamento dovrebbe tenere conto dei diritti e delle libertà delle persone fisiche in linea con le prescrizioni di cui all'articolo 5, paragrafo 1, lettera e).

Il titolare del trattamento dovrebbe inoltre assicurarsi che i dati rimangano aggiornati durante il periodo di conservazione in maniera da ridurre il rischio di inesattezze[11].

B. BASI LEGITTIME PER IL TRATTAMENTO

Il processo decisionale automatizzato di cui all'articolo 22, paragrafo 1, è consentito soltanto qualora si applichi una delle eccezioni di cui al capitolo IV (se-

zioni C e D). Le seguenti basi legittime per il trattamento sono pertinenti per tutti i processi decisionali automatizzati relativi alle persone fisiche e di profilazione.

1. ARTICOLO 6, PARAGRAFO 1, LETTERA A) - CONSENSO

Il consenso come base per il trattamento in generale è trattato nelle Linee guida del Gruppo di lavoro sul consenso[12]. Il consenso esplicito è una delle eccezioni al divieto di processo decisionale automatizzato e profilazione di cui all'articolo 22, paragrafo 1.

La profilazione può non essere trasparente. Spesso si basa su dati derivati o desunti da altri dati, anziché su dati forniti direttamente dall'interessato.

Il titolare del trattamento che intende fare affidamento sul consenso come base per la profilazione dovrà dimostrare che gli interessati comprendono esattamente a cosa stanno acconsentendo e dovrà ricordare che il consenso non è sempre una base appropriata per il trattamento[13]. In tutti i casi, gli interessati dovrebbero disporre di sufficienti informazioni pertinenti sull'uso previsto e sulle conseguenze del trattamento in maniera da assicurare che il consenso fornito sia frutto di una scelta informata.

2. ARTICOLO 6, PARAGRAFO 1, LETTERA B) - NECESSARIO ALL'ESECUZIONE DI UN CONTRATTO

Il titolare del trattamento potrebbe voler utilizzare la profilazione e i processi decisionali automatizzati perché tali processi:

- consentono potenzialmente una maggiore coerenza o correttezza nel processo decisionale (ad esempio riducendo le possibilità di errore umano, discriminazione e abuso di potere);
- riducono il rischio che i clienti non riescano a soddisfare i pagamenti per beni o servizi (ad esempio utilizzando referenze per il credito), o
- consentono di prendere decisioni in tempi più brevi e migliorare l'efficienza.

Indipendentemente da quanto sopra, queste considerazioni da sole non sono sufficienti a dimostrare che questo tipo di trattamento è *necessario* ai sensi dell'articolo 6, paragrafo 1, lettera b), per l'esecuzione di un contratto. Come descritto nel parere del Gruppo di lavoro sull'interesse legittimo[14], la nozione di necessità deve essere interpretata in maniera restrittiva.

Quello che segue è un esempio di profilazione che *non* soddisfa le condizioni di cui all'articolo 6, paragrafo 1, lettera b).

Esempio

Un utente acquista alcuni articoli da un rivenditore al dettaglio online. Per soddisfare il contratto, il rivenditore deve trattare le informazioni della carta di credito dell'utente per finalità di pagamento e l'indirizzo dell'utente per consegnare la merce. Il completamento del contratto non dipende dalla creazione di un profilo dei gusti e delle scelte in termini di stile di vita dell'utente, basato sulle sue visite sul sito web. Anche se la profilazione è espressamente menzionata in caratteri minuscoli nel contratto, questo fatto, da solo, non la rende "necessaria" all'esecuzione del contratto.

3. ARTICOLO 6, PARAGRAFO 1, LETTERA C) - NECESSARIO PER ADEMPIERE UN OBBLIGO LEGALE

Vi possono essere casi in cui sussiste un obbligo legale[15] all'esecuzione della profilazione, ad esempio in relazione alla prevenzione delle frodi o al riciclaggio di denaro. Il parere del Gruppo di lavoro sugli interessi legittimi[16] fornisce informazioni utili su questa base per il trattamento e sulle garanzie da applicare.

4. ARTICOLO 6, PARAGRAFO 1, LETTERA D) - NECESSARIO PER LA SALVAGUARDIA DI INTERESSI VITALI

Tale base si applica nelle circostanze in cui il trattamento è necessario per la salvaguardia di un interesse essenziale per la vita dell'interessato o di un'altra persona fisica.

Determinati tipi di trattamento possono essere necessari per importanti motivi di interesse pubblico e per proteggere gli interessi vitali dell'interessato, come la profilazione per sviluppare modelli che individuino in anticipo la diffusione di malattie potenzialmente letali o in situazioni di emergenza umanitaria. In questi casi, tuttavia, e in linea di principio, il titolare del trattamento può basarsi su motivi di interesse vitale unicamente se non sono disponibili altre basi giuridiche per il trattamento[17]. Se il trattamento comprende dati personali appartenenti a categorie particolari, il titolare del trattamento deve altresì assicurarsi di soddisfare le prescrizioni di cui all'articolo 9, paragrafo 2, lettera c).

5. ARTICOLO 6, PARAGRAFO 1, LETTERA E) - NECESSARIO PER L'ESECUZIONE DI UN COMPITO DI INTERESSE PUBBLICO O CONNESSO ALL'ESERCIZIO DI PUBBLICI POTERI

L'articolo 6, paragrafo 1, lettera e), potrebbe costituire una base adeguata per la profilazione nel settore pubblico in determinate circostanze. Il compito o la funzione devono avere una base giuridica chiara.

6. ARTICOLO 6, PARAGRAFO 1, LETTERA F) - NECESSARIO PER IL PERSEGUIMENTO DEL LEGITTIMO INTERESSE[18] DEL TITOLARE DEL TRATTAMENTO O DI TERZI

La profilazione è consentita se è necessaria ai fini degli interessi legittimi[19] perseguiti dal titolare del trattamento o da un terzo. Tuttavia, l'articolo 6, paragrafo 1, lettera f), non si applica automaticamente soltanto perché il titolare del trattamento o il terzo ha un legittimo interesse. Il titolare del trattamento deve procedere a una ponderazione per valutare se gli interessi o i diritti e le libertà fondamentali dell'interessato non prevalgano sui propri interessi.

I seguenti aspetti sono particolarmente rilevanti:

- il livello di dettaglio del profilo (un interessato profilato in un gruppo descritto in maniera ampia come "persone interessate alla letteratura inglese" o segmentato e mirato a livello granulare);
- la completezza del profilo (il profilo descrive solo un aspetto minore dell'interessato oppure dipinge un quadro più completo);
- l'impatto della profilazione (gli effetti sull'interessato);
- le garanzie destinate ad assicurare la correttezza, la non discriminazione e l'esattezza nel processo di profilazione.

Sebbene si basi sull'articolo 7 della direttiva 95/46/CE sulla protezione dei dati, il parere del Gruppo di lavoro sui legittimi interessi[20] contiene esempi che sono comunque utili e pertinenti per il titolare del trattamento che svolge attività di profilazione. Tale parere suggerisce inoltre che sarebbe difficile per il titolare del trattamento giustificare il ricorso al legittimo interesse come base legittima per pratiche intrusive di profilazione e tracciamento per finalità di marketing o pubblicità, ad esempio quelle che comportano il tracciamento di persone fisiche su più siti web, ubicazioni, dispositivi, servizi o l'intermediazione di dati.

Nel valutare la validità del trattamento ai sensi dell'articolo 6, paragrafo 1, lettera f), il titolare del trattamento dovrebbe altresì considerare l'uso futuro o la combinazione di profili.

C. ARTICOLO 9 - CATEGORIE PARTICOLARI DI DATI

Il titolare del trattamento può trattare dati personali appartenenti a categorie particolari soltanto se ricorrono una delle condizioni di cui all'articolo 9, paragrafo 2, e una condizione di cui all'articolo 6. Questo vale anche per i dati appartenenti a categorie particolari derivati o desunti da attività di profilazione.

La profilazione può creare dati appartenenti a categorie particolari desumendoli da dati che di per sé non appartengono a categorie particolari ma che diventano tali se combinati con altri dati. Ad esempio, può essere possibile desumere lo stato di salute di una persona associando le registrazioni dei suoi acquisti di alimenti a dati sulla qualità e sul contenuto energetico di tali alimenti.

Possono essere scoperte correlazioni che forniscono indicazioni sulla salute, sulle convinzioni politiche o religiose oppure sull'orientamento sessuale delle persone, come dimostrato dal seguente esempio:

Esempio

Uno studio[21] ha combinato i "Mi Piace" di Facebook con informazioni limitate tratte da sondaggi e ha rilevato che i ricercatori hanno predetto con precisione l'orientamento sessuale di un utente maschile nell'88 % dei casi, l'origine etnica di un utente nel 95 % dei casi e se un utente era cristiano o musulmano nell'82 % dei casi.

Se dalla profilazione sono dedotte preferenze e caratteristiche sensibili, il titolare del trattamento dovrebbe assicurarsi:

- che il trattamento non sia incompatibile con la finalità originaria;
- di aver individuato una base legittima per il trattamento di dati appartenenti a categorie particolari;
- di informare l'interessato sul trattamento.

Il processo decisionale automatizzato, così come descritto dall'articolo 22, paragrafo 1, basato su categorie particolari di dati, è trattato nel capitolo IV (sezione D).

D. DIRITTI DELL'INTERESSATO[22]

Il regolamento introduce maggiori diritti per gli interessati e crea nuovi obblighi per i titolari del trattamento.

Nel contesto della profilazione questi diritti possono essere esercitati nei confronti del titolare del trattamento che crea il profilo e del titolare del trattamento che prende una decisione automatizzata su un interessato (con o senza intervento umano), qualora tali soggetti non siano il medesimo.

Esempio

Un intermediario di dati effettua la profilazione di dati personali. In linea con gli obblighi di cui agli articoli 13 e 14, deve informare l'interessato in merito al trattamento e al fatto che intende condividere il profilo con altre organizzazioni. Deve inoltre indicare separatamente anche i dettagli relativi al diritto di opposizione di cui all'articolo 21, paragrafo 1.

L'intermediario di dati condivide il profilo con un'altra impresa. Tale impresa utilizza il profilo per inviare alla persona in questione comunicazioni di marketing diretto.

L'impresa deve informare l'interessato [articolo 14, paragrafo 1, lettera c)] in merito alle finalità dell'utilizzo del profilo e alla fonte da cui ha ottenuto l'in-

formazione [articolo 14, paragrafo 2, lettera f)] nonché al diritto dell'interessato di opporsi al trattamento, compresa la profilazione, per finalità di marketing diretto (articolo 21, paragrafo 2).

L'intermediario di dati e l'impresa devono consentire all'interessato di accedere alle informazioni utilizzate (articolo 15) per correggere eventuali informazioni errate (articolo 16) e, in determinate circostanze, di cancellare il profilo o i dati personali utilizzati per crearlo (articolo 17). L'interessato deve inoltre ricevere informazioni sul proprio profilo, ad esempio, in merito ai "segmenti" o alle "categorie" nei quali viene collocato[23].

Se utilizza il profilo per prendere una decisione basata unicamente sul trattamento automatizzato che produce effetti giuridici o che incide in modo analogo significativamente sull'interessato, l'impresa è soggetta alle disposizioni dell'articolo 22. (Ciò non esclude l'intermediario di dati dall'articolo 22 se il trattamento soddisfa la soglia pertinente).

1. ARTICOLI 13 E 14 - DIRITTO DI ESSERE INFORMATO

In considerazione del principio fondamentale della trasparenza che sta alla base del regolamento, il titolare del trattamento deve spiegare in maniera chiara e semplice alle persone interessate come funziona la profilazione o il processo decisionale automatizzato.

In particolare, quando il trattamento implica un processo decisionale basato sulla profilazione (indipendentemente dal fatto che rientri nell'applicazione delle disposizioni di cui all'articolo 22), deve essere chiarito all'interessato[24] il fatto che il trattamento avviene per finalità di a) profilazione e di b) adozione di decisioni basate sul profilo generato.

Il considerando 60 afferma che fornire informazioni sulla profilazione fa parte degli obblighi di trasparenza del titolare del trattamento ai sensi dell'articolo 5, paragrafo 1, lettera a). L'interessato ha diritto di *essere informato* dal titolare del trattamento e, in alcune circostanze, gode di un diritto di *opposizione alla* "profilazione", *indipendentemente* del fatto che abbia luogo un processo decisionale unicamente automatizzato relativo alle persone fisiche.

Ulteriori orientamenti sulla trasparenza in generale[25] sono disponibili nelle Linee guida del Gruppo di lavoro sulla trasparenza ai sensi del regolamento.

2. ARTICOLO 15 - DIRITTO DI ACCESSO

L'articolo 15 conferisce all'interessato il diritto di ottenere informazioni dettagliate sui dati personali utilizzati per la profilazione, ivi comprese le categorie di dati impiegati per creare un profilo.

Oltre alle informazioni generali sul trattamento, ai sensi dell'articolo 15, paragrafo 3, il titolare del trattamento deve rendere disponibili i dati utilizzati come input per creare il profilo, e consentire l'accesso alle informazioni sul profilo e ai dettagli dei segmenti nei quali l'interessato è stato inserito.

Ciò differisce dal diritto alla portabilità dei dati di cui all'articolo 20, nel contesto del quale il titolare del trattamento è tenuto soltanto a comunicare i dati forniti dall'interessato o osservati dal titolare del trattamento e non il profilo stesso[26].

Il considerando 63 offre una certa protezione al titolare del trattamento nei confronti della divulgazione di segreti aziendali o proprietà intellettuale, che può essere particolarmente pertinente in relazione alla profilazione. Tale considerando afferma che il diritto di accesso "non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software". Tuttavia, il titolare del trattamento non può fare affidamento sulla protezione dei segreti aziendali come scusa per negare l'accesso o rifiutarsi di fornire informazioni all'interessato.

Il considerando 63 specifica inoltre che "ove possibile, il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali".

3. ARTICOLO 16 - DIRITTO DI RETTIFICA; ARTICOLO 17 - DIRITTO ALLA CANCELLAZIONE; ARTICOLO 18 - DIRITTO DI LIMITAZIONE DI TRATTAMENTO

La profilazione può comportare un elemento di previsione, il che aumenta il rischio di inesattezza. I dati di input possono essere inesatti o irrilevanti oppure avulsi dal contesto. L'algoritmo utilizzato per individuare le correlazioni potrebbe presentare lacune.

Il diritto di rettifica di cui all'articolo 16 potrebbe applicarsi, ad esempio, nel caso in cui una persona venga inserita in una categoria che esprime un giudizio sulla propria capacità di eseguire un compito, e tale profilo sia basato su informazioni errate. Le persone potrebbero voler contestare l'esattezza dei dati utilizzati e qualsiasi raggruppamento o categoria che è stata loro applicata.

I diritti di rettifica e di cancellazione[27] si applicano tanto ai "dati personali di input" (i dati personali utilizzati per creare il profilo) quanto ai "dati di output" (il profilo stesso o il "punteggio" assegnato alla persona fisica).

L'articolo 16 prevede altresì il diritto dell'interessato di integrare i dati personali con informazioni aggiuntive.

Esempio

Il sistema informatico di un centro medico locale colloca una persona in un gruppo che presenta maggiori probabilità di sviluppare malattie cardiache. Questo "profilo" non è necessariamente impreciso nonostante tale persona non abbia mai sofferto di malattie cardiache.

Il profilo afferma semplicemente che la persona in questione ha *maggiori probabilità* di sviluppare malattie cardiache. Ciò può essere di fatto corretto, in termini statistici.

Ciò nonostante l'interessato ha il diritto, tenendo conto della finalità del trattamento, di fornire una dichiarazione integrativa. Nella fattispecie, la dichiarazione potrebbe essere basata, ad esempio, su un sistema informatico medico (e su un modello statistico) più avanzato che include nel calcolo dati aggiuntivi e svolge esami più dettagliati rispetto a quello del centro medico locale con capacità più limitate.

Il diritto di limitazione di trattamento (articolo 18) si applica a qualsiasi fase del processo di profilazione.

4. ARTICOLO 21 - DIRITTO DI OPPOSIZIONE

Il titolare del trattamento deve portare *espressamente* all'attenzione dell'interessato informazioni dettagliate in merito al diritto di opposizione di cui all'articolo 21, paragrafi 1 e 2, e presentare tale diritto chiaramente e separatamente da qualsiasi altra informazione (articolo 21, paragrafo 4).

Ai sensi dell'articolo 21, paragrafo 1, l'interessato può opporsi al trattamento (compresa la profilazione), per motivi connessi alla sua situazione particolare. Il titolare del trattamento è specificamente tenuto a riconoscere tale diritto in tutti i casi nei quali il trattamento si basi sull'articolo 6, paragrafo 1, lettere e) o f).

Dopo che l'interessato ha esercitato questo diritto, il titolare del trattamento deve interrompere[28] (o evitare di iniziare) il processo di profilazione, a meno che non possa dimostrare l'esistenza di motivi legittimi cogenti che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato. Il titolare del trattamento potrebbe altresì dover cancellare i dati personali pertinenti[29].

Il regolamento non fornisce alcuna spiegazione di motivi che sarebbero considerati motivi legittimi cogenti[30]. Può accadere, ad esempio, che la profilazione sia utile per la società in senso lato (o per la comunità più ampia) e non soltanto per gli interessi aziendali del titolare del trattamento, come nel caso della profilazione volta a individuare in anticipo la diffusione di malattie contagiose.

Il titolare del trattamento dovrebbe:

- considerare l'importanza della profilazione per il proprio particolare obiettivo;
- considerare l'impatto della profilazione sugli interessi, sui diritti e sulle libertà dell'interessato, che dovrebbe essere limitato al minimo necessario per conseguire l'obiettivo;
- procedere a una ponderazione.

È sempre necessario procedere a una ponderazione tra gli interessi concorrenti del titolare del trattamento e la base per l'opposizione dell'interessato (che può fondarsi su motivi personali, sociali o professionali). A differenza della direttiva 95/46/CE, l'onere della prova di dimostrare l'esistenza di motivi legittimi cogenti spetta al titolare del trattamento e non all'interessato.

Dalla formulazione dell'articolo 21 risulta evidente che la ponderazione differisce da quella di cui all'articolo 6, paragrafo 1, lettera f). In altre parole, non è sufficiente che il titolare del trattamento dimostri soltanto che la sua precedente analisi dell'interesse legittimo era corretta, occorre inoltre che detto interesse legittimo sia *cogente*, il che implica una soglia maggiore per prevalere rispetto alle opposizioni.

L'articolo 21, paragrafo 2, riconosce all'interessato un diritto *incondizionato* ad opporsi al trattamento dei suoi dati personali per finalità di marketing diretto, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto[31]. Ciò significa che non è necessario effettuare alcun bilanciamento degli interessi; il titolare del trattamento deve rispettare le volontà dell'interessato senza mettere in discussione i motivi dell'opposizione. Il considerando 70 fornisce ulteriore contesto a questo diritto e afferma che può essere esercitato in qualsiasi momento e gratuitamente.

IV. DISPOSIZIONI SPECIFICHE RELATIVE A DECISIONI BASATE UNICAMENTE SUL TRATTAMENTO AUTOMATIZZATO DI CUI ALL'ARTICOLO 22

L'articolo 22, paragrafo 1, afferma che:

> l'interessato ha il diritto di non essere sottoposto a una decisione *basata unicamente* sul trattamento automatizzato, compresa la profilazione, che produca *effetti giuridici* che lo riguardano o che *incida in modo analogo significativamente sulla sua persona*.

Il termine "diritto" contenuto nella disposizione non significa che l'articolo 22, paragrafo 1, si applica soltanto se invocato attivamente dall'interessato. L'articolo 22, paragrafo 1, stabilisce un divieto generale nei confronti del processo decisionale basato unicamente sul trattamento automatizzato. Tale divieto si applica indipendentemente dal fatto che l'interessato intraprenda un'azione in merito al trattamento dei propri dati personali.

In sintesi, l'articolo 22 stabilisce che:

I) di norma, esiste un divieto generale all'adozione di decisioni completamente automatizzate relative alle persone fisiche, compresa la profilazione, che hanno un effetto giuridico o che incidono in modo analogo significativamente;
II) esistono eccezioni alla regola;
III) laddove si applichi una di tali eccezioni, devono essere adottate misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato[32].

Questa interpretazione sostiene l'idea secondo la quale l'interessato deve avere il controllo sui propri dati personali, in linea con i principi fondamentali del regolamento. Interpretare l'articolo 22 come un divieto piuttosto che come un diritto da invocare significa che le persone sono automaticamente protette dagli effetti potenziali che questo tipo di trattamento può avere. La formulazione dell'articolo suggerisce che questa è l'intenzione, sostenuta anche dal considerando 71, che afferma:

> tuttavia, **è opportuno che sia consentito** adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri (...), o se è necessario per la conclusione o l'esecuzione di un contratto (...), o se l'interessato ha espresso il proprio consenso esplicito.

Ciò implica che il trattamento ai sensi dell'articolo 22, paragrafo 1, non è consentito in generale[33].

Tuttavia il divieto di cui all'articolo 22, paragrafo 1 si applica esclusivamente in circostanze specifiche quando una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, ha un effetto giuridico o incide in modo analogo significativamente su una persona, come spiegato ulteriormente nelle linee guida. Anche in questi casi esistono precise eccezioni che consentono l'esecuzione di tale trattamento.

Le garanzie richieste, discusse in maggior dettaglio in appresso, comprendono il diritto di essere informati (di cui agli articoli 13 e 14 – informazioni specificamente significative sulla logica utilizzata, nonché sull'importanza e sulle conseguenze previste per l'interessato) e garanzie, quali il diritto di ottenere l'intervento umano e il diritto di contestare la decisione (di cui all'articolo 22, paragrafo 3).

Qualsiasi trattamento che possa presentare un rischio elevato per gli interessati impone al titolare del trattamento di svolgere una valutazione d'impatto sulla protezione dei dati[34]. Oltre ad affrontare qualsiasi altro rischio connesso al trattamento, una valutazione d'impatto sulla protezione dei dati può essere particolarmente utile per i titolari del trattamento che non sono certi che le attività da loro proposte rientrino nella definizione di cui all'articolo 22, pa-

ragrafo 1, e, laddove tali attività siano consentite da un'eccezione individuata, non sappiano quali garanzie debbano essere applicate.

A. "DECISIONE BASATA UNICAMENTE SUL TRATTAMENTO AUTOMATIZZATO"

L'articolo 22, paragrafo 1, si riferisce a decisioni "basate unicamente" sul trattamento automatizzato.
Ciò significa che non vi è alcun coinvolgimento umano nel processo decisionale.

Esempio

Un processo automatizzato produce ciò che di fatto è una raccomandazione riguardante un interessato. Se un essere umano riesamina il risultato del processo automatizzato e tiene conto di altri fattori nel prendere la decisione finale, tale decisione non sarà "basata unicamente" sul trattamento automatizzato.

Il titolare del trattamento non può eludere le disposizioni dell'articolo 22 creando coinvolgimenti umani fittizi. Ad esempio, se qualcuno applica abitualmente profili generati automaticamente a persone fisiche senza avere alcuna influenza effettiva sul risultato, si tratterà comunque di una decisione basata unicamente sul trattamento automatico.

Per aversi un coinvolgimento umano, il titolare del trattamento deve garantire che qualsiasi controllo della decisione sia significativo e non costituisca un semplice gesto simbolico. Il controllo dovrebbe essere effettuato da una persona che dispone dell'autorità e della competenza per modificare la decisione. Nel contesto dell'analisi, tale persona dovrebbe prendere in considerazione tutti i dati pertinenti.

Nell'ambito della valutazione d'impatto sulla protezione dei dati, il titolare del trattamento dovrebbe individuare e registrare il grado di coinvolgimento umano nel processo decisionale e la fase nella quale quest'ultimo ha luogo.

B. EFFETTI "GIURIDICI" O "IN MODO ANALOGO SIGNIFICATIVI"

Il regolamento riconosce che il processo decisionale automatizzato, compresa la profilazione, può avere gravi conseguenze per le persone fisiche. Il regolamento non definisce i concetti di "giuridico" o "in modo analogo significativi", tuttavia la formulazione dell'articolo 22 chiarisce che rientreranno nell'applicazione dell'articolo soltanto gli effetti che hanno un impatto grave.

"DECISIONE CHE PRODUCE EFFETTI GIURIDICI"

Un effetto giuridico richiede che la decisione, basata unicamente su un trattamento automatico, incida sui diritti giuridici di una persona, quali la libertà di

associarsi ad altre persone, di votare nel contesto di un'elezione o di intraprendere azioni legali. Un effetto giuridico può altresì essere qualcosa che influisce sullo status giuridico di una persona o sui suoi diritti ai sensi di un contratto. Tra gli esempi di questo tipo di effetto figurano le decisioni automatizzate su una persona fisica che portano:

- alla cancellazione di un contratto;
- alla concessione o alla negazione del diritto a una particolare prestazione sociale concessa dalla legge, come l'indennità di alloggio o le prestazioni per figli a carico;
- al rifiuto dell'ammissione in un paese o la negazione della cittadinanza.

"INCIDA IN MODO ANALOGO SIGNIFICATIVAMENTE SULLA SUA PERSONA"

Anche se un processo decisionale non ha effetto sui diritti giuridici delle persone, potrebbe comunque rientrare nell'ambito di applicazione dell'articolo 22 se produce un effetto equivalente o in modo analogo significativo in termini di impatto.

In altre parole, anche qualora non vi sia alcun cambiamento nei suoi diritti od obblighi giuridici, l'interessato potrebbe comunque subire ripercussioni sufficienti da richiedere le protezioni previste da questa disposizione. Il regolamento introduce l'espressione "in modo analogo" (non presente nell'articolo 15 della direttiva 95/46/CE) associandola a "incida significativamente". Di conseguenza la soglia per l'*importanza* deve essere analoga a quella di una decisione che produce un effetto giuridico.

Il considerando 71 fornisce i seguenti esempi tipici: "rifiuto automatico di una domanda di credito online" o "pratiche di assunzione elettronica senza interventi umani".

Affinché il trattamento dei dati sia considerato incidere in maniera significativa su una persona, i suoi effetti devono essere sufficientemente rilevanti o importanti da meritare attenzione. In altre parole, la decisione deve poter essere in grado di:

- incidere in maniera significativa sulle circostanze, sul comportamento o sulle scelte dell'interessato;
- avere un impatto prolungato o permanente sull'interessato; o
- nel caso più estremo, portare all'esclusione o alla discriminazione di persone.

È difficile essere precisi su ciò che può essere considerato sufficientemente significativo per il raggiungimento della soglia, sebbene le seguenti decisioni possano rientrare in tale categoria:

- decisioni che influenzano le circostanze finanziarie di una persona, come la sua ammissibilità al credito;
- decisioni che influenzano l'accesso di una persona ai servizi sanitari;
- decisioni che negano a una persona un'opportunità di impiego o pongono tale persona in una posizione di notevole svantaggio;
- decisioni che influenzano l'accesso di una persona all'istruzione, ad esempio le ammissioni universitarie.

Ciò conduce anche al problema della pubblicità online, che si basa sempre più su strumenti automatizzati e implica decisioni basate unicamente sul trattamento automatizzato. Oltre al soddisfacimento delle disposizioni generali del regolamento, trattate nel capitolo III, possono essere pertinenti anche le disposizioni della proposta di regolamento sulla vita privata e le comunicazioni elettroniche. Inoltre, i minori richiedono una protezione maggiore, come sarà esaminato in appresso nel capitolo V.

In numerosi casi tipici, la decisione di proporre pubblicità mirata basata sulla profilazione non inciderà in modo analogo significativamente sulle persone, ad esempio nel caso di una pubblicità per un outlet di moda online basato su un semplice profilo demografico: "donne nella regione di Bruxelles di età compresa tra 25 e 35 che potrebbero essere interessate alla moda e ad alcuni capi di abbigliamento".

Tuttavia è possibile che ciò possa accadere, a seconda delle particolari caratteristiche del caso, tra le quali:

- l'invasività del processo di profilazione, compreso il tracciamento delle persone su siti web, dispositivi e servizi diversi;
- le aspettative e le volontà delle persone interessate;
- il modo in cui viene reso disponibile l'annuncio pubblicitario; o
- lo sfruttamento della conoscenza di vulnerabilità degli interessati coinvolti.

Un trattamento che potrebbe avere un impatto minimo sulle persone in generale potrebbe in effetti incidere in maniera significativa su taluni gruppi della società, quali gruppi minoritari o adulti vulnerabili. Ad esempio, una persona di cui sono note le difficoltà finanziarie, effettive o potenziali, e che riceve regolarmente annunci pubblicitari di prestiti ad alto interesse potrebbe sottoscrivere tali offerte e incorrere così in ulteriori debiti.

Anche un processo decisionale automatizzato che si traduce in una fissazione dei prezzi differenziata basata su dati personali o caratteristiche personali potrebbe incidere in maniera significativa se, ad esempio, prezzi proibitivi elevati impediscono effettivamente a una persona di ottenere determinati beni o servizi.

Analogamente, effetti significativi possono risultare anche da azioni di persone diverse dalla persona alla quale fa riferimento la decisione automatizzata. Un'illustrazione di questo caso è riportata in appresso.

Esempio

Ipoteticamente, una società che fornisce carte di credito potrebbe ridurre il limite della carta di un cliente non sulla base dello storico dei rimborsi di quel cliente, bensì su criteri di credito non tradizionali, quali un'analisi di altri clienti che vivono nella medesima area e acquistano presso i medesimi negozi.

Ciò potrebbe comportare la limitazione delle opportunità di una persona sulla base di azioni di terzi.

In un contesto diverso, il ricorso a questi tipi di caratteristiche potrebbe avere il vantaggio di estendere il credito a coloro che non hanno una storia creditizia convenzionale, alle quali sarebbe altrimenti negato l'accesso.

C. ECCEZIONI AL DIVIETO

L'articolo 22, paragrafo 1, stabilisce un divieto generale all'adozione di un processo decisionale unicamente automatizzato relativo alle persone fisiche con effetti giuridici o che incidono in modo analogo significativamente, come descritto sopra.

Di conseguenza il titolare del trattamento non dovrebbe intraprendere il trattamento descritto nell'articolo 22, paragrafo 1, a meno che non si applichi una delle seguenti eccezioni di cui all'articolo 22, paragrafo 2, nel contesto delle quali la decisione:

a) è necessaria per la conclusione o l'esecuzione di un contratto;
b) è autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; o
c) si basa sul consenso esplicito dell'interessato.

Laddove il processo decisionale coinvolga categorie particolari di dati definite all'articolo 9, paragrafo 1, il titolare del trattamento deve altresì garantire di poter soddisfare i requisiti di cui all'articolo 22, paragrafo 4.

1. ESECUZIONE DI UN CONTRATTO

Il titolare del trattamento potrebbe voler ricorrere a processi decisionali basati unicamente sul trattamento automatizzato per finalità contrattuali ritenendo che sia il modo più appropriato per conseguire l'obiettivo. Talvolta il coinvolgimento umano di routine può essere impraticabile o impossibile in ragione della notevole quantità di dati che vengono trattati.

Il titolare del trattamento deve essere in grado di dimostrare che questo tipo di trattamento è necessario, tenendo conto della possibilità di adottare un metodo più rispettoso della vita privata[35]. Se esistono altri mezzi efficaci e meno invasivi per il conseguimento del medesimo obiettivo, allora il trattamento non sarà "necessario".

Il processo decisionale automatizzato di cui all'articolo 22, paragrafo 1, può essere necessario anche per un trattamento precontrattuale.

Esempio

Un'azienda pubblicizza un posto di lavoro vacante. Essendo il posto molto ambito, l'azienda riceve decine di migliaia di candidature. In ragione del volume eccezionalmente elevato di candidature l'azienda potrebbe ritenere che non è possibile individuare i candidati idonei senza prima utilizzare mezzi unicamente automatizzati per scartare le candidature non pertinenti. In questo caso potrebbe essere necessario ricorrere a un processo decisionale automatizzato per stilare un elenco ristretto di possibili candidati allo scopo di stipulare un contratto con un interessato.

Il capitolo III (sezione B) fornisce maggiori informazioni sui contratti come base legittima per il trattamento.

2. AUTORIZZATO DAL DIRITTO DELL'UNIONE O DELLO STATO MEMBRO

Il processo decisionale automatizzato, compresa la profilazione, potrebbe potenzialmente aver luogo ai sensi dell'articolo 22, paragrafo 2, lettera b), se il diritto dell'Unione o dello Stato membro ne autorizza l'uso. La legislazione pertinente deve altresì prevedere misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Il considerando 71 afferma che tale trattamento potrebbe includere il ricorso al processo decisionale automatizzato di cui all'articolo 22, paragrafo 1, per fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale o a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento.

3. CONSENSO ESPLICITO

L'articolo 22 richiede il consenso esplicito. Il trattamento che rientra nella definizione di cui all'articolo 22, paragrafo 1, pone rischi significativi in termini di protezione dei dati e pertanto si ritiene opportuno un livello elevato di controllo individuale sui dati personali.

Il "consenso esplicito" non è definito nel regolamento; tuttavia le linee guida

del Gruppo di lavoro sul consenso[36] forniscono orientamenti in merito alla sua interpretazione.

Il capitolo III (sezione B) fornisce maggiori informazioni sul consenso in generale.

D. CATEGORIE PARTICOLARI DI DATI PERSONALI - ARTICOLO 22, PARAGRAFO 4

Il processo decisionale automatizzato (di cui all'articolo 22, paragrafo 1) che comporta l'uso di categorie particolari di dati personali è consentito soltanto se sono soddisfatte le seguenti condizioni cumulative (articolo 22, paragrafo 4):

- esiste un'esenzione applicabile in virtù dell'articolo 22, paragrafo 2;
- si applicano la lettera a) o g) dell'articolo 9, paragrafo 2.

Articolo 9, paragrafo 2, lettera a) - consenso esplicito dell'interessato; o

Articolo 9, paragrafo 2, lettera g) - trattamento necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

In entrambi i casi di cui sopra, il titolare del trattamento deve altresì adottare misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

E. DIRITTI DELL'INTERESSATO[37]

1. ARTICOLO 13, PARAGRAFO 2, LETTERA F), E ARTICOLO 14, PARAGRAFO 2, LETTERA G) - DIRITTO DI ESSERE INFORMATO

In considerazione dei potenziali rischi e delle interferenze che la profilazione di cui all'articolo 22 pone in relazione ai diritti degli interessati, il titolare del trattamento dovrebbe prestare particolare attenzione agli obblighi in materia di trasparenza.

L'articolo 13, paragrafo 2, lettera f), e l'articolo 14, paragrafo 2, lettera g), impongono al titolare del trattamento di fornire informazioni specifiche e facilmente accessibili sul processo decisionale automatizzato, basato unicamente sul trattamento automatizzato,. compresa la profilazione, che produce effetti giuridici o in modo analogo significativi[38].
Se prende decisioni automatizzate come descritto nell'articolo 22, paragrafo 1, il titolare del trattamento deve:

- comunicare all'interessato che sta svolgendo tale tipo di attività;
- fornire informazioni significative sulla logica utilizzata;
- spiegare l'importanza e le conseguenze previste di tale trattamento.

Fornire queste informazioni aiuterà altresì il titolare del trattamento a garantire il rispetto di talune garanzie obbligatorie di cui all'articolo 22, paragrafo 3, e al considerando 71.

Se il processo decisionale automatizzato e la profilazione non soddisfano la definizione di cui all'articolo 22, paragrafo 1, è comunque buona prassi fornire le informazioni di cui sopra. In ogni caso il titolare del trattamento deve fornire informazioni sufficienti all'interessato in maniera da rendere il trattamento corretto[39] e soddisfare tutti gli altri requisiti in materia di informazione di cui agli articoli 13 e 14.

INFORMAZIONI SIGNIFICATIVE SULLA "LOGICA UTILIZZATA"

La crescita e la complessità dell'apprendimento automatico possono rendere difficile comprendere come funzionano un processo decisionale automatizzato o la creazione di profili.

Il titolare del trattamento dovrebbe trovare modi semplici per comunicare all'interessato la logica o i criteri sui quali si basa l'adozione della decisione. Il regolamento impone al titolare del trattamento di fornire informazioni significative sulla logica utilizzata, ma non necessariamente una spiegazione complessa degli algoritmi utilizzati o la divulgazione dell'algoritmo completo[40]. Le informazioni fornite dovrebbero tuttavia essere sufficientemente complete affinché l'interessato possa comprendere i motivi alla base della decisione.

Esempio

Un titolare del trattamento utilizza il punteggio di affidabilità creditizia *(credit scoring)* per valutare e respingere una domanda di prestito di una persona. Tale punteggio può essere stato fornito da un'agenzia di referenze per il credito oppure calcolato direttamente sulla base delle informazioni detenute dal titolare del trattamento.

Indipendentemente dalla fonte (le informazioni sulla fonte devono essere fornite all'interessato ai sensi dell'articolo 14, paragrafo 2, lettera f), qualora i dati personali non siano stati ottenuti dall'interessato), se il titolare del trattamento si basa su tale punteggio, deve essere in grado di spiegarlo e di illustrarne la logica all'interessato.

Il titolare del trattamento spiega che tale processo lo aiuta a prendere decisioni corrette e responsabili in merito ai prestiti concessi. Fornisce dettagli sulle principali caratteristiche considerate per giungere alla decisione, sulla fonte di tali informazioni e sulla loro importanza. Ciò può includere, ad esempio:

- informazioni fornite dall'interessato nel modulo di domanda;
- informazioni sulla situazione anteriore del conto, compresi eventuali pagamenti arretrati;
- informazioni derivanti da registri pubblici ufficiali, quali i registri di frodi e i registri d'insolvenza.

Il titolare del trattamento include altresì informazioni per spiegare all'interessato che i metodi di valutazione del grado di affidabilità creditizia utilizzati sono sottoposti a verifiche regolari per garantire che rimangano corretti, efficaci ed esenti da distorsioni.

Il titolare del trattamento fornisce i dati di contatto affinché l'interessato possa chiedere il riesame di qualsiasi decisione respinta, in linea con le disposizioni di cui all'articolo 22, paragrafo 3.

"IMPORTANZA" E "CONSEGUENZE PREVISTE"

Questi termini suggeriscono che devono essere fornite informazioni sul trattamento previsto o futuro, nonché sulle possibili conseguenze del processo decisionale automatizzato sull'interessato[41]. Per rendere queste informazioni significative e comprensibili, dovrebbero essere forniti esempi reali e concreti del tipo di possibili effetti.

In un contesto digitale, il titolare del trattamento potrebbe essere in grado di utilizzare strumenti aggiuntivi per illustrare tali effetti.

Esempio

Una compagnia assicurativa utilizza un processo decisionale automatizzato per definire i premi assicurativi per gli autoveicoli in funzione del comportamento di guida dei clienti. Per illustrare il significato e le conseguenze previste del trattamento, la compagnia spiega che una guida pericolosa può comportare premi assicurativi più elevati e fornisce un'applicazione che confronta conducenti fittizi, tra i quali uno con abitudini di guida pericolose come rapide accelerazioni e frenate all'ultimo minuto.

Usa elementi grafici per dare consigli su come migliorare tali abitudini e, di conseguenza, su come ridurre i premi assicurativi.

Il titolare del trattamento può utilizzare tecniche visive simili per spiegare come è stata presa una decisione nel passato.

2. ARTICOLO 15, PARAGRAFO 1, LETTERA H) - DIRITTO DI ACCESSO

L'articolo 15, paragrafo 1, lettera h), riconosce agli interessati il diritto di disporre delle medesime informazioni in merito a una decisione basata uni-

camente sul trattamento automatizzato, compresa la profilazione, rispetto a quelle previste dall'articolo 13, paragrafo 2, lettera f), e dall'articolo 14, paragrafo 2, lettera g), ossia:

- l'esistenza di processi decisionali automatizzati, compresa la profilazione;
- informazioni significative sulla logica utilizzata;
- l'importanza e le conseguenze previste del trattamento per l'interessato.

Il titolare del trattamento, dovrebbe aver già fornito tali dati all'interessato in linea con gli obblighi di cui all'articolo 13[42].

L'articolo 15, paragrafo 1, lettera h), afferma che il titolare del trattamento deve fornire all'interessato informazioni sulle conseguenze previste del trattamento, piuttosto che una spiegazione di una particolare decisione. Il considerando 63 chiarisce questo aspetto affermando che ogni interessato dovrebbe avere il diritto di accesso al fine di ottenere "comunicazioni" sul trattamento automatizzato dei dati, compresa la logica in questione e, almeno quando è basato sulla profilazione, sulle conseguenze del trattamento.

Esercitando i diritti di cui all'articolo 15, l'interessato può prendere atto di una decisione presa nei suoi confronti, ivi compresa una decisione basata sulla profilazione.

Il titolare del trattamento dovrebbe fornire all'interessato informazioni di carattere generale (in particolare, sui fattori presi in considerazione per il processo decisionale e sul rispettivo "peso" a livello aggregato) che sono utili all'interessato anche per contestare la decisione.

F. STABILIRE GARANZIE ADEGUATE

Se la base per il trattamento è l'articolo 22, paragrafo 2, lettera a), oppure l'articolo 22, paragrafo 2, lettera c), l'articolo 22, paragrafo 3 impone al titolare del trattamento di attuare misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi degli interessati. Ai sensi dell'articolo 22, paragrafo 2, lettera b), il diritto degli Stati membri o dell'Unione che autorizza il trattamento deve altresì prevedere misure di adeguate di tutela.

Tali misure dovrebbero includere quanto meno la possibilità per l'interessato di ottenere l'intervento umano, esprimere il proprio punto di vista e contestare la decisione.

L'intervento umano è un aspetto fondamentale. Qualsiasi riesame dovrebbe essere effettuato da una persona che dispone dell'autorità e della competenza adeguate per modificare la decisione. Il responsabile di tale riesame dovrebbe effettuare una valutazione approfondita di tutti i dati pertinenti, comprese eventuali informazioni aggiuntive fornite dall'interessato.

Il considerando 71 sottolinea che in *ogni caso* le garanzie adeguate dovrebbero comprendere anche:

> la specifica informazione all'interessato e il diritto (...) di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione.

Il titolare del trattamento deve mettere a disposizione dell'interessato un modo semplice per esercitare tali diritti.

Ciò sottolinea la necessità di trasparenza del trattamento. L'interessato sarà in grado di contestare una decisione o esprimere il proprio parere soltanto se comprende pienamente come è stata presa la decisione e su quali basi. I requisiti in materia di trasparenza sono discussi nel capitolo IV (sezione E).

Errori o distorsioni nei dati raccolti o condivisi oppure un errore o una distorsione nel processo decisionale automatizzato possono comportare:

- classificazioni errate e
- valutazioni basate su proiezioni imprecise, che
- incidono negativamente sulle persone fisiche.

Il titolare del trattamento dovrebbe effettuare valutazioni frequenti degli insiemi di dati che tratta, in maniera da rilevare eventuali distorsioni, e sviluppare metodi per affrontare eventuali elementi pregiudizievoli, compreso un eccessivo affidamento sulle correlazioni.

I sistemi che verificano gli algoritmi e i riesami periodici dell'esattezza e della pertinenza del processo decisionale automatizzato, compresa la profilazione, sono ulteriori misure utili.

Il titolare del trattamento dovrebbe introdurre procedure e misure adeguate per prevenire errori, inesattezze[43] o discriminazioni sulla base di categorie particolari di dati. Queste misure dovrebbero essere attuate ciclicamente; non soltanto in fase di progettazione, ma anche in continuativamente, durante l'applicazione della profilazione alle persone fisiche. L'esito di tali verifiche dovrebbe andare ad alimentare nuovamente la progettazione del sistema.

Ulteriori esempi di garanzie adeguate sono riportati nella sezione dedicata alle raccomandazioni.

V. MINORI E PROFILAZIONE

Il regolamento introduce ulteriori obblighi per il titolare del trattamento qualora tratti dati personali di minori.

L'articolo 22 di per sé non opera alcuna distinzione in merito al fatto che il trattamento riguardi adulti o minori. Tuttavia, il considerando 71 afferma che

le decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, che producono effetti giuridici o in modo analogo significativi non dovrebbero riguardare minori[44]. Dato che tale formulazione non si riflette nell'articolo stesso, il Gruppo di lavoro non ritiene che ciò rappresenti un divieto assoluto di questo tipo di trattamento in relazione ai minori. Tuttavia, alla luce di tale considerando, il Gruppo di lavoro raccomanda ali titolare del trattamento di non fare affidamento, di norma, sulle eccezioni di cui all'articolo 22, paragrafo 2, per giustificare tale trattamento.

Potrebbero tuttavia esservi talune circostanze nelle quali è necessario che il titolare del trattamento prenda decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, aventi effetti giuridici o in modo analogo significativi in relazione ai minori, ad esempio per tutelarne il benessere. In tal caso, il trattamento può essere effettuato sulla base delle eccezioni di cui all'articolo 22, paragrafo 2, lettere a), b) o c), a seconda dei casi.

In questi casi devono essere messe in atto garanzie adeguate, come previsto dall'articolo 22, paragrafo 2, lettera b), e dall'articolo 22, paragrafo 3, e devono pertanto essere appropriate per i minori. Il titolare del trattamento deve garantire che tali garanzie siano efficaci nel tutelare i diritti, le libertà e i legittimi interessi dei minori i cui dati vengono trattati.

L'esigenza di una tutela particolare nei confronti dei minori si riflette nel considerando 38 il quale afferma che:

> i minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di *marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore*.

L'articolo 22 non impedisce al titolare del trattamento di prendere decisioni basate unicamente sul trattamento automatizzato in relazione ai minori, se tali decisioni non avranno un effetto giuridico o in modo analogo significativo sul minore. Tuttavia, una decisione basata unicamente sul trattamento automatizzato che influenza le scelte e il comportamento di un minore potrebbe potenzialmente avere un effetto giuridico o in modo analogo significativo sullo stesso, a seconda della natura delle scelte e dei comportamenti in questione.

Dato che i minori rappresentano un gruppo più vulnerabile della società, le organizzazioni dovrebbero, in generale, astenersi dal profilarli per finalità di marketing[45]. I minori possono essere particolarmente vulnerabili nell'ambiente online e più facilmente influenzabili dalla pubblicità comportamentale. Ad esempio, nei giochi online, la profilazione può servire per individuare i gioca-

tori che l'algoritmo ritiene più propensi a spendere soldi, oltre a fornire annunci più personalizzati. L'età e la maturità del minore possono influenzarne la capacità di comprendere la motivazione che sta alla base di tale tipo di marketing o le sue conseguenze[46].

L'articolo 40, paragrafo 2, lettera g), fa esplicitamente riferimento alla preparazione di codici di condotta che includano misure per la protezione dei minori; potrebbe altresì essere possibile integrare i codici esistenti[47].

VI. VALUTAZIONI D'IMPATTO SULLA PROTEZIONE DEI DATI E RESPONSABILE DELLA PROTEZIONE DEI DATI

La responsabilizzazione è un aspetto importante e un requisito esplicito ai sensi del regolamento[48].

In quanto strumento essenziale per la responsabilizzazione, la valutazione d'impatto sulla protezione dei dati consente al titolare del trattamento di valutare i rischi connessi al processo decisionale automatizzato, compresa la profilazione. Essa permette di dimostrare che sono state messe in atto misure adeguate per affrontare tali rischi e dimostrare il rispetto del regolamento.

L'articolo 35, paragrafo 3, lettera a), sottolinea la necessità che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati in caso di:

> *una valutazione sistematica e globale* di aspetti personali relativi a persone fisiche, *basata su* un trattamento automatizzato, *compresa* la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche.

L'articolo 35, paragrafo 3, lettera a), fa riferimento a valutazioni comprendenti la profilazione e decisioni che sono "basate" su un trattamento automatizzato, piuttosto che basate "unicamente" su un trattamento automatizzato. Ciò significa che l'articolo 35, paragrafo 3, lettera a), si applicherà sia a un processo decisionale che comprenda la profilazione e abbia effetti giuridici o in modo analogo significativi che non è un processo decisionale interamente automatizzato, sia a una decisione basata unicamente sul trattamento automatizzato di cui all'articolo 22, paragrafo 1.

Se il titolare del trattamento prevede un "modello" in cui adotta decisioni basate unicamente su un trattamento automatizzato aventi un *impatto elevato* sulle persone fisiche, fondate su profili relativi a queste ultime, e *non può* fare affidamento sul consenso di dette persone, su un contratto stipulato con le stesse o su una legge che autorizza tale trattamento, il titolare del trattamento non dovrebbe procedere.

Il titolare del trattamento può comunque prevedere un "modello" di processo decisionale basato sulla profilazione, aumentando significativamente il livello

di intervento umano affinché detto modello *non sia più un processo decisionale interamente automatizzato*, sebbene il trattamento possa comunque presentare rischi per i diritti e le libertà fondamentali delle persone. In tal caso, il titolare del trattamento deve assicurarsi di riuscire a far fronte a tali rischi e soddisfare i requisiti esposti al capitolo III delle presenti linee guida.

Una valutazione d'impatto sulla protezione dei dati può altresì costituire uno strumento utile a disposizione del titolare del trattamento per individuare le misure che introdurrà per far fronte ai rischi per la protezione dei dati connessi al trattamento. Tali misure[49] potrebbero comprendere:

- informare l'interessato dell'esistenza e della logica utilizzata nel processo decisionale automatizzato;
- spiegare l'importanza e le conseguenze previste del trattamento per l'interessato;
- fornire all'interessato i mezzi per opporsi alla decisione;
- consentire all'interessato di esprimere il proprio punto di vista.

Ulteriori attività di profilazione possono giustificare una valutazione d'impatto sulla protezione dei dati, a seconda delle circostanze del caso. Il titolare del trattamento può consultare le linee guida del Gruppo di lavoro sulle valutazioni d'impatto sulla protezione dei dati[50] per ulteriori informazioni e per contribuire a determinare la necessità di effettuare una valutazione d'impatto sulla protezione dei dati.

Un requisito aggiuntivo in termini di responsabilizzazione consiste nella designazione di un responsabile della protezione dei dati, nei casi in cui la profilazione e/o il processo decisionale automatizzato costituiscono un'attività centrale del titolare del trattamento e richiedono un monitoraggio regolare e sistematico degli interessati su larga scala (articolo 37, paragrafo 1, lettera b)[51].

ALLEGATO 1
RACCOMANDAZIONI SULLE BUONE PRASSI

Le seguenti raccomandazioni sulle buone prassi aiuteranno il titolare del trattamento a soddisfare i requisiti stabiliti dalle disposizioni del regolamento generale sulla protezione dei dati in materia di profilazione e processo decisionale automatizzato[52].

Articolo	Questione	Raccomandazione
5, paragrafo 1, lettera a); 12, 13, 14	Diritto di ottenere informazioni	Il titolare del trattamento dovrebbe consultare le linee guida del Gruppo di lavoro sulla trasparenza (WP 260) per i requisiti generali in materia di trasparenza. Oltre ai requisiti generali, quando tratta dati in linea con l'articolo 22, il titolare del trattamento deve fornire informazioni significative sulla logica utilizzata. Anziché fornire una complessa spiegazione matematica su come funzionano gli algoritmi o l'apprendimento automatico, il titolare del trattamento dovrebbe prendere in considerazione l'utilizzo di metodi chiari ed esaustivi per fornire informazioni all'interessato, ad esempio: • categorie di dati che sono state o saranno utilizzate nella profilazione o nel processo decisionale; • motivi per i quali tali categorie sono considerate pertinenti; • modalità di creazione del profilo utilizzato nel processo decisionale automatizzato, ivi comprese le statistiche utilizzate nell'analisi; • motivi per i quali tale profilo è pertinente per il processo decisionale automatizzato; • modalità di utilizzo del profilo ai fini di una decisione riguardante l'interessato. Tali informazioni saranno di norma più pertinenti per l'interessato e contribuiranno alla trasparenza del trattamento.

		Il titolare del trattamento potrebbe prendere in considerazione tecniche di visualizzazione e interattive in maniera da favorire la trasparenza degli algoritmi[53].
6 paragrafo 1, lettera a)	Consenso come base per il trattamento	Se si fonda sul consenso come base per il trattamento, il titolare del trattamento dovrebbe consultare le Linee guida del Gruppo di lavoro sul consenso (WP 259).
15	Diritto di accesso	Il titolare del trattamento potrebbe prendere in considerazione l'attuazione di un meccanismo che consenta agli interessati di verificare il loro profilo, compresi i dettagli delle informazioni e le fonti utilizzate per svilupparlo.
16	Diritto di rettifica	Il titolare del trattamento che fornisce agli interessati accesso al loro profilo nel rispetto dei loro diritti di cui all'articolo 15 dovrebbe consentire agli stessi di aggiornare o modificare eventuali inesattezze presenti nei dati o nel profilo. Ciò può altresì aiutare il titolare del trattamento a rispettare gli obblighi di cui all'articolo 5, paragrafo 1, lettera d). Il titolare del trattamento potrebbe prendere in considerazione la possibilità di introdurre strumenti di gestione delle preferenze online, ad esempio un dashboard per la protezione dei dati, permettendo così agli interessati di gestire l'uso delle loro informazioni in una serie di servizi diversi, consentendo loro di modificare le impostazioni, aggiornare i loro dettagli personali e rivedere o modificare il loro profilo per correggere eventuali inesattezze.
Articolo 21, paragrafi 1 e 2	Diritto di opposizione	Il diritto di opposizione di cui all'articolo 21, paragrafi 1 e 2, deve essere esplicitamente portato a conoscenza dell'interessato e presentato chiaramente e separatamente da altre informazioni (articolo 21, paragrafo 4). Il titolare del trattamento deve garantire che tale diritto venga visualizzato in maniera visibile sul suo sito web o in qualsiasi documentazione pertinente e non sia nascosto all'interno di altre condizioni generali di contratto/servizio.

22 e considerando 71	Garanzie adeguate	L'elenco che segue, sebbene non esaustivo, fornisce alcuni suggerimenti di buone prassi che il titolare del trattamento dovrebbe tenere in considerazione quando prende decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione (definite all'articolo 22, paragrafo 1): • controlli regolari di garanzia della qualità dei sistemi per assicurare che le persone siano trattate in maniera equa e non siano discriminate sulla base di categorie particolari di dati personali o in altro modo; • verifica degli algoritmi – testare gli algoritmi utilizzati e sviluppati dai sistemi di apprendimento automatico per dimostrare che stanno effettivamente funzionando come previsto e non producono risultati discriminatori, errati o ingiustificati; • per l'audit indipendente di "terzi" (laddove il processo decisionale basato sulla profilazione abbia un impatto elevato sulle persone fisiche), fornitura all'ispettore di tutte le informazioni necessarie su come funziona l'algoritmo o il sistema di apprendimento automatico; • per gli algoritmi di terzi, ottenimento di garanzie contrattuali che sono stati effettuati audit e test e che l'algoritmo è conforme alle norme concordate; • misure specifiche per la minimizzazione dei dati al fine di prevedere periodi di conservazione chiari per i profili e per tutti i dati personali utilizzati durante la creazione o l'applicazione dei profili; • utilizzo di tecniche di anonimizzazione o pseudonimizzazione nel contesto della profilazione; • modi per consentire all'interessato di esprimere il proprio punto di vista e contestare la decisione;

		• un meccanismo per l'intervento umano in determinati casi, ad esempio fornendo un collegamento a una procedura di ricorso nel momento in cui la decisione automatizzata viene trasmessa all'interessato, con termini concordati per il riesame e la designazione di un punto di contatto per qualsiasi domanda. Il titolare del trattamento può altresì valutare opzioni quali: • meccanismi di certificazione per i trattamenti; • codici di condotta per la verifica dei processi che comportano apprendimento automatico; • comitati di revisione etica per valutare i potenziali danni e benefici per la società di particolari applicazioni per la profilazione.

ALLEGATO 2
PRINCIPALI DISPOSIZIONI DEL REGOLAMENTO

Principali disposizioni del regolamento che fanno riferimento alla profilazione e al processo decisionale automatizzato in generale

Articolo	Considerando	Osservazioni
3, paragrafo 2, lettera b)	24	Il monitoraggio del comportamento [degli interessati] nella misura in cui tale comportamento ha luogo all'interno dell'Unione. **Considerando 24:** " (...) tracciate su internet (...) ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, *in particolare per adottare decisioni* che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali".
4, paragrafo 4	30	**Articolo 4, paragrafo 4** definizione di profilazione **Considerando 30:** "identificativi online (...), quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza (...) possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, *possono essere utilizzate per creare profili delle persone fisiche e identificarle"*.
5 e 6	72	**Considerando 72** "la profilazione è soggetta alle norme del presente regolamento che disciplinano il trattamento dei dati personali, quali le basi giuridiche del trattamento **(articolo 6)** o i principi di protezione dei dati **(articolo 5)**".
8	38	Utilizzo dei dati personali dei minori per la profilazione. **Considerando 38:** "I minori meritano una specifica protezione (...) in particolare [in merito al]l'utilizzo dei dati personali dei minori a fini di (...) creazione di profili di personalità o di utente".

13 e 14	60	Diritto di essere informato. **Considerando 60:** "inoltre l'interessato *[deve] essere informato dell'esistenza di una profilazione e delle conseguenze della stessa"*.
15	63	Diritto di accesso. **Considerando 63:** "diritto di conoscere e ottenere comunicazioni (...) in relazione alla finalità per cui i dati personali sono trattati (...) e, *almeno* quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento".
21, paragrafi 1, 2 e 3	70	Diritto di opposizione alla profilazione. **Considerando 70:** "(...) il diritto (...) di opporsi a tale trattamento (...), compresa la profilazione nella misura in cui sia connessa a tale marketing diretto".
23	73	**Considerando 73:** "il diritto dell'Unione o degli Stati membri può imporre limitazioni a specifici principi e (...) al diritto di opporsi, alle decisioni basate sulla profilazione (...), ove ciò sia necessario e proporzionato in una società democratica (...)" per la tutela di obiettivi specifici di interesse pubblico generale.
35, paragrafo 3, lettera a)	91	Una valutazione d'impatto sulla protezione dei dati è necessaria nel caso di una "valutazione sistematica e globale di aspetti personali relativi a persone fisiche, *basata* su un trattamento automatizzato, che include la profilazione, e in base al quale si adottano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche". **Riguarda il processo decisionale, compresa la profilazione, che è non si basa unicamente su un trattamento automatizzato.**

Principali disposizioni del regolamento che fanno riferimento al processo decisionale automatizzato di cui all'articolo 22

13, paragrafo 2, lettera f) e 14, paragrafo 2, lettera g	61	Diritto di essere informato in merito a: • esistenza di processi decisionali automatizzati ai sensi dell'**articolo 22, paragrafi 1 e 4**; • informazioni significative sulla logica utilizzata; • importanza e conseguenze previste del trattamento.
15, lettera h)		Diritti di accesso specifici alle informazioni sull'esistenza di un processo decisionale unicamente automatizzato, compresa la profilazione.
22, paragrafo 1	71	Divieto di processo decisionale basato unicamente sul trattamento automatizzato, compresa la profilazione, che produce effetti giuridici/in modo analogo significativi. Oltre alla spiegazione fornita nel corpo principale delle linee guida, i seguenti punti ampliano la logica per la lettura dell'articolo 22 come un divieto: • sebbene il capo III riguardi i diritti dell'interessato, le disposizioni di cui agli articoli 12-22 non riguardano esclusivamente l'esercizio *attivo* di diritti. Taluni dei diritti sono *passivi*; non si riferiscono tutti a situazioni nelle quali l'interessato intraprende un'azione, ovvero effettua una richiesta o un reclamo o una domanda di qualche tipo. Gli articoli 15-18 e 20-21 riguardano l'interessato che esercita attivamente i suoi diritti, mentre gli articoli 13 e 14 riguardano i doveri che il titolare del trattamento deve adempiere senza alcun coinvolgimento attivo dell'interessato. Di conseguenza l'inclusione dell'articolo 22 in tale capo non significa di per sé che si tratti di un diritto di opposizione; • l'articolo 12, paragrafo 2, riguarda l'esercizio dei "diritti dell'interessato" ai sensi degli articoli da 15 a 22; ma ciò non significa che l'articolo 22, paragrafo

		1 stesso debba essere interpretato come un diritto. All'articolo 22 vi *è* un diritto attivo, tuttavia esso rientra nelle garanzie che devono essere applicate nei casi in cui è consentito il processo decisionale automatizzato [articolo 22, paragrafo 2, lettere da a) a c)] - il diritto di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione. Si applica soltanto in tali casi, poiché è vietato lo svolgimento del trattamento descritto nell'articolo 22, paragrafo 1, su altre basi; • l'articolo 22 si trova in una sezione del regolamento denominata "Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche", il che implica che l'articolo 22 *non* contiene un diritto di opposizione come l'articolo 21. Ciò è ulteriormente sottolineato dalla mancanza nell'articolo 22 di un obbligo di informazione esplicitamente equivalente a quello di cui all'articolo 21, paragrafo 4; • se l'articolo 22 dovesse essere interpretato come un diritto di opposizione, l'eccezione di cui all'articolo 22, paragrafo 2, lettera c), non avrebbe molto senso. L'eccezione afferma che il processo decisionale automatizzato può comunque avere luogo se l'interessato ha fornito il proprio consenso esplicito (cfr. in appresso). Ciò sarebbe contraddittorio in quanto l'interessato non può opporsi e acconsentire al medesimo trattamento; • un'opposizione comporterebbe l'obbligo di eseguire l'intervento umano. Le eccezioni di cui all'articolo 22, paragrafo 2, lettere a) e c), prevalgono sulla norma principale di cui all'articolo 22, paragrafo 1, tuttavia soltanto fino a quando l'intervento umano è disponibile per l'interessato, come specificato all'articolo 22, paragrafo 3. Poiché l'interessato (opponendosi) ha già richiesto l'intervento umano, l'articolo 22, paragrafo 2, lettere a) e c), sarebbe automaticamente eluso in ogni caso, rendendo così tali lettere prive di significato.

		Considerando 71: "(...) Tale trattamento comprende la 'profilazione', che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (...) *"Tale misura non dovrebbe riguardare un minore"*.
22, paragrafo 2, lettere da a) a c)	71	**L'articolo 22, paragrafo 2** deroga al divieto di trattamento basato: **a)** sull'esecuzione o la stipula di un contratto; **b)** sul diritto dell'Unione o degli Stati membri; o **c)** sul consenso esplicito **considerando 71** fornisce ulteriore contesto in merito all'**articolo 22, paragrafo 2, lettera b)**, e afferma che il trattamento descritto all'**articolo 22, paragrafo 1:** "se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento (...)".
22, paragrafo 3	71	**L'articolo 22, paragrafo 3 e il considerando 71** specificano inoltre che anche nei casi di cui all'**articolo 22, paragrafo 2, lettere a)** e **c)**, il trattamento dovrebbe essere soggetto a garanzie adeguate. **Considerando 71:** "che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore".

23	73	**Considerando 73:** "il diritto dell'Unione o degli Stati membri può imporre limitazioni a specifici principi e (...) al diritto di opporsi, alle decisioni basate sulla profilazione (...), ove ciò sia necessario e proporzionato in una società democratica (...)" per la tutela di obiettivi specifici di interesse pubblico generale.
35, paragrafo 3, lettera a)	91	Come va svolta una valutazione d'impatto sulla protezione dei dati?
47, paragrafo 2, lettera e)	71	Norme vincolanti d'impresa di cui **all'articolo 47, paragrafo 1,** dovrebbero specificare almeno "(...) il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione ai sensi dell'**articolo 22** (...)".

ALLEGATO 3
APPROFONDIMENTI

Le presenti linee guida tengono conto di quanto segue:

- Gruppo di lavoro, Documento di consulenza sugli elementi essenziali di una definizione e una disposizione sulla profilazione nel contesto del regolamento generale sulla protezione dei dati dell'UE, adottato il 13 maggio 2013 (in inglese);
- Gruppo di lavoro, Parere 2/2010 sulla pubblicità comportamentale online, WP 171;
- Gruppo di lavoro, Parere 03/2013 sulla limitazione della finalità, WP 203 (in inglese);
- Gruppo di lavoro, Parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE, WP 217;
- Gruppo di lavoro, Dichiarazione sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati, WP 218, (in inglese);
- Gruppo di lavoro, Parere 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti, WP 223;
- Gruppo di lavoro, Linee guida sui responsabili della protezione dei dati, WP 243;
- Gruppo di lavoro, Linee guida per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento, WP 244;
- Gruppo di lavoro, Linee guida sul consenso, WP 259 (in inglese);
- Gruppo di lavoro, Linee guida sulla trasparenza, WP 260 (in inglese);
- Consiglio d'Europa. Raccomandazione CM/Rec (2010)13 sulla protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione;
- Consiglio d'Europa. *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 01/2017 (in inglese);
- Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection version 2.0, 03/2017 (in inglese);
- Office of the Australian Commissioner - *Consultation draft: Guide to big data and the Australian Privacy Principles,* 05/2016 (in inglese);
- Garante europeo della protezione dei dati (GEPD) Parere 7/2015 – *Meeting the challenges of big data,* 19 novembre 2015 (in inglese);
- Datatilsynet – *Big Data – privacy principles under pressure* 09/2013 (in inglese);
- Consiglio d'Europa. Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale - Progetto di re-

lazione esplicativa sulla versione modernizzata della convenzione 108 del CdE, agosto 2016 (in inglese);

- Datatilsynet – *The Great Data Race – How commercial utilisation of personal data challenges privacy. Report*, novembre 2015 (in inglese);
- Garante europeo della protezione dei dati – *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit* (in inglese);
- Comitato congiunto delle autorità europee di vigilanza. *Joint Committee Discussion Paper on the use of Big Data by financial institutions* 2016-86 (in inglese). https://www.esma.europa.eu/sites/default/files/library/jc-2016-86_discussion_paper_big_data.pdf;
- Commission de la protection de la vie privée. *Big Data Rapport* https://www.privacycommission.be/sites/privacycommission/files/documents/Big%20Data%20vo or%20MindMap%2022-02-17%20fr.pdf;
- Senato degli Stati Uniti, Comitato per il commercio, la scienza e i trasporti. *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, rapporto informativo per il presidente Rockefeller, 18 dicembre 2013 (in inglese). https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf;
- Lilian Edwards e Michael Veale. *Slave to the Algorithm? Why a 'Right to an Explanation' is probably not the remedy you are looking for* (in inglese). Documento di ricerca, pubblicato il 24 maggio 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855;
- NYTimes.com. *Showing the Algorithms behind New York City Services*. https://mobile.nytimes.com/2017/08/24/nyregion/showing-the-algorithms-behind-new-york-city-services.html?referer=https://t.co/6uUVVjOIXx?amp=1. Accesso effettuato il 24 agosto 2017;
- Consiglio d'Europa. Raccomandazione CM/REC (2018)x del Comitato dei Ministri agli Stati membri sugli orientamenti per promuovere, proteggere e adempiere i diritti dei minori https://wwwnell'ambientedigitale.coe.int/en/web/children/(progettoriveduto,25-/calllug-iofor2017)-consultation(ininglese)-guidelines.-for-member-states-to-promote-protect-and-fulfil-children-s-rights-in- the-digital-environment?inheritRedirect=true&redirect=%2Fen%2Fweb%2Fchildren. Accesso effettuato il 31 agosto 2017;
- Unicef. *Privacy, protection of personal information and reputation rights. Discussion paper series: Children's Rights and Business in a Digital World* (in inglese). https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf. Accesso effettuato il 31 agosto 2017;
- Camera dei Lord. *Growing up with the internet*. Select Committee on Communications, Seconda relazione delle sessioni 2016-2017 (in inglese). https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/13002.htm. Accesso effettuato il 31 agosto 2017;

- Sandra Wachter, Brent Mittelstadt e Luciano Floridi. *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, 28 dicembre 2016 (in inglese). https://www.turing.ac.uk/research_projects/data-ethics-group-deg/. Accesso effettuato il 13 dicembre 2017;
- Sandra Wachter, Brent Mittelstadt e Chris Russell. *Counterfactual explanations Without Opening the Black Box: Automated Decisions and the GDPR*, 6 ottobre 2017 (in inglese). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289. Accesso effettuato il 13 dicembre 2017;
- Governo australiano. *Better Practice Guide, Automated Assistance in Administrative Decision-Making. Six steps methodology, plus summary of checklist points Part 7*, febbraio 2007 (in inglese). https://www.oaic.gov.au/images/documents/migrated/migrated/betterpracticeguide.pdf. Accesso effettuato il 9 gennaio 2018.

NOTE

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE. La profilazione e il processo decisionale automatizzato relativo alle persone fisiche sono disciplinati anche dalla direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati. Sebbene si concentrino sulla profilazione e sul processo decisionale automatizzato relativo alle persone fisiche ai sensi del regolamento generale sulla protezione dei dati, le presenti linee guida sono rilevanti anche per quanto riguarda le disposizioni analoghe su questi due temi contenute nella direttiva 2016/680. Le caratteristiche specifiche della profilazione e del processo decisionale automatizzato relativo alle persone fisiche ai sensi della direttiva 2016/680 sono analizzate nel parere WP 258 "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)" [Parere su alcune questioni chiave della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie], adottato dal Gruppo di lavoro il 29 novembre 2017, che tratta tali aspetti alle pagine 11-14. Tale parere è disponibile (in inglese) all'indirizzo: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178.

[2] Consiglio d'Europa. La protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione. Raccomandazione CM/Rec (2010)13 e relazione. Consiglio d'Europa, 23 novembre 2010. https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf. Accesso effettuato il 24 aprile 2017;

[3] Come stabilito all'articolo 22, paragrafo 1, del regolamento generale sulla protezione dei dati.

[4] Regolamento generale sulla protezione dei dati, considerando 72: "la profilazione è soggetta alle norme del presente regolamento che disciplinano il trattamento dei dati personali, quali le basi giuridiche del trattamento o i principi di protezione dei dati".

[5] Le linee guida del Gruppo di lavoro in materia di trasparenza trattano della trasparenza in modo più approfondito; cfr. "Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)" [Linee guida sulla trasparenza ai sensi del regolamento (UE) 2016/679], 11 aprile 2018 (in inglese) http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

[6] Ufficio del commissario australiano per l'informazione. Bozza di consultazione: Guide to big data and the Australian Privacy Principles [Guida ai megadati e ai principi australiani in materia di tutela della vita privata], 05/2016. In tale documento si afferma che: "le informative sulla protezione dei dai personali devono comunicare le informazioni relative alle prassi applicate in maniera chiara e semplice, nonché esaustiva e con sufficiente specificità da poter essere significative. La stessa tecnologia che porta a una maggiore raccolta di informazioni personali offre anche l'opportunità di realizzare informative sulla protezione dei dati più dinamiche, a più livelli e incentrate sull'utente". https://www.oaic.gov.au/engage-with-us/consultations/

guide-to-big-data-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacy-principles. Accesso effettuato il 24 aprile 2017.

[7] Questo esempio è tratto da: Senato degli Stati Uniti, Comitato per il commercio, la scienza e i trasporti. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes [Rassegna del settore degli intermediari: raccolta, utilizzo e vendita di dati sui consumatori per finalità di marketing], rapporto informativo per il presidente Rockefeller, 18 dicembre 2013 (in inglese). https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Cfr. pagina ii della sintesi e pagina 12 del corpo principale del documento. Accesso effettuato il 21 luglio 2017.

[8] Si noti che possono trovare applicazione anche le disposizioni del futuro regolamento sulla vita privata e le comunicazioni elettroniche.

[9] Evidenziati nel documento del Gruppo di lavoro "Opinion 03/2013 on purpose limitation" [Parere 03/2013 sulla limitazione della finalità], 2 aprile 2013 (in inglese). http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Accesso effettuato il 24 aprile 2017.

[10] Articolo 6, paragrafo 4, del regolamento generale sulla protezione dei dati.

[11] Autorità norvegese di protezione dei dati. "The Great Data Race – How commercial utilisation of personal data challenges privacy" [La corsa ai dati eccezionali – Quali sono le sfide in termini di tutela della vita privata poste dall'utilizzo commerciale di dati personali], relazione, novembre 2015. Datatilsynet https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/. Accesso effettuato il 24 aprile 2017.

[12] Gruppo di lavoro articolo 29, Linee guida sul consenso ai sensi del regolamento (UE) 2016/679, 28 novembre 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Accesso effettuato il 18 dicembre 2017.

[13] Ibidem.

[14] Parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE. Commissione europea, 9 aprile 2014. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf. Accesso effettuato il 24 aprile 2017.

[15] Considerando 41 e 45 del regolamento generale sulla protezione dei dati.

[16] Pagina 22 Gruppo di lavoro articolo 29, Parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE. Commissione europea, 9 aprile 2014. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf. Accesso effettuato il 24 aprile 2017.

[17] Considerando 46 del regolamento generale sulla protezione dei dati.

[18] I legittimi interessi elencati nel considerando 47 del regolamento comprendono il trattamento per finalità di marketing diretto e il trattamento strettamente necessario a fini di prevenzione delle frodi.

[19] Il "legittimo interesse" del titolare del trattamento non può rendere lecita la profilazione se il trattamento rientra nella definizione di cui all'articolo 22, paragrafo 1.

[20] Gruppo di lavoro articolo 29, Parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE. Commissione europea, 9 aprile 2014, pagina 55, esempi alle pagine 70 e 71. http://ec.europa.eu/justice/article-29/documentation/

opinion-recommendation/files/2014/wp217_it.pdf. Accesso effettuato il 24 aprile 2017.

[21] Michael Kosinski, David Stilwell e Thore Graepel. Private traits and attributes are predictable from digital records of human behaviour [Tratti e attributi privati sono prevedibili dalle registrazioni digitali del comportamento umano]. Atti della National Academy of Sciences degli Stati Uniti d'America, http://www.pnas.org/content/110/15/5802.full.pdf. Accesso effettuato il 29 marzo 2017.

[22] La presente sezione è pertinente tanto per la profilazione quanto per il processo decisionale automatizzato. Per il processo decisionale automatizzato ai sensi dell'articolo 22, si ricorda che esistono anche requisiti aggiuntivi come descritto nel capitolo IV.

[23] Autorità norvegese di protezione dei dati. "The Great Data Race - How commercial utilisation of personal data challenges privacy". Relazione, novembre 2015. https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/. Accesso effettuato il 24 aprile 2017.

[24] Articolo 13, paragrafo 1, lettera c), e articolo 14, paragrafo 1, lettera c), del regolamento generale sulla protezione dei dati. L'articolo 13, paragrafo 2, lettera f), e l'articolo 14, paragrafo 2, lettera g), impongono al titolare del trattamento di informare l'interessato dell'esistenza di un processo decisionale automatizzato, compresa la profilazione, di cui all'articolo 22, paragrafi 1 e 4. Questo aspetto è spiegato ulteriormente nel capitolo IV.

[25] Gruppo di lavoro articolo 29, Linee guida sulla trasparenza ai sensi del regolamento (UE) 2016/679 (WP 260), 28 novembre 2017 (in inglese) http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850, Accesso effettuato il 18 dicembre 2017.

[26] Pagina 9 del documento del Gruppo di lavoro, Linee guida sul diritto alla portabilità dei dati, WP 242 https://www.garanteprivacy.it/documents/10160/5184810/Linee-guida+sul+diritto+alla+portabilit%C3%A0+dei+dati+-+WP+242.pdf. Accesso effettuato il 8 gennaio 2018.

[27] Articolo 17 del regolamento generale sulla protezione dei dati.

[28] Articolo 18, paragrafo 1, lettera d), del regolamento.

[29] Articolo 17, paragrafo 1, lettera c), del regolamento.

[30] Cfr. la spiegazione di legittimità nel documento del Gruppo di lavoro "Parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE". 9 aprile 2014. Pagine 28-31. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf. Accesso effettuato il 24 aprile 2017.

[31] In linea con l'articolo 12, paragrafo 2, il titolare del trattamento che raccoglie dati personali da persone fisiche allo scopo di utilizzarli per finalità di marketing diretto dovrebbe, al momento della raccolta, considerare la possibilità di offrire agli interessati un modo semplice per indicare che non desiderano che i loro dati personali siano utilizzati per finalità di marketing diretto, anziché richiedere loro di esercitare il diritto di opposizione in un secondo momento.

[32] Il considerando 71 afferma che tale trattamento dovrebbe essere "subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione".

[33] Ulteriori commenti sull'interpretazione dell'articolo 22 come divieto sono riportati nell'allegato 2.

[34] Gruppo di lavoro articolo 29, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determi-

nazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento 2016/679. 4 aprile 2017. Commissione europea. https://www.garanteprivacy.it/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati. Accesso effettuato il 24 aprile 2017.

[35] Buttarelli, Giovanni. Assessing the necessity of measures that limit the fundamental right to the protection of personal data. A Toolkit [Valutazione della necessità di misure che limitano il diritto fondamentale alla protezione dei dati personali. Uno strumentario]. Garante europeo della protezione dei dati, 11 aprile 2017, (in inglese) https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf. Accesso effettuato il 24 aprile 2017.

[36] Gruppo di lavoro articolo 29, Linee guida sul consenso ai sensi del regolamento 2016/679, WP 259. 28 novembre 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Accesso effettuato il 18 dicembre 2017.

[37] L'articolo 12 del regolamento stabilisce le modalità applicabili all'esercizio dei diritti dell'interessato.

[38] Di cui all'articolo 22, paragrafi 1 e 4. Le linee guida del Gruppo di lavoro sulla trasparenza trattano dei requisiti generali in materia di informazione di cui agli articoli 13 e 14.

[39] Considerando 60 del regolamento: "il titolare del trattamento dovrebbe fornire all'interessato eventuali ulteriori informazioni necessarie ad assicurare un trattamento corretto e trasparente, prendendo in considerazione le circostanze e del contesto specifici in cui i dati personali sono trattati Inoltre l'interessato dovrebbe essere informato dell'esistenza di una profilazione e delle conseguenze della stessa".

[40] La complessità non è una scusa per non fornire informazioni all'interessato. Il considerando 58 afferma che il principio di trasparenza è "particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online".

[41] Consiglio d'Europa. Draft Explanatory Report on the modernised version of CoE Convention 108 [Progetto di relazione esplicativa sulla versione modernizzata della convenzione 108 del CdE], punto 75: "gli interessati dovrebbero avere il diritto di conoscere il ragionamento alla base del trattamento dei loro dati, nonché le conseguenze di tale ragionamento, che ha portato a conclusioni conclusive, in particolare nei casi che prevedono l'uso di algoritmi per il processo decisionale automatizzato, compresa la profilazione. Ad esempio nel caso del grado di affidabilità creditizia, gli interessati dovrebbero avere il diritto di conoscere la logica alla base del trattamento dei loro dati risultante in una decisione "sì" o "no" e non semplicemente informazioni sulla decisione stessa. In assenza di comprensione di questi aspetti non potrebbe esserci alcun effettivo esercizio di altre garanzie essenziali quali il diritto di opposizione e il diritto di proporre reclami presso un'autorità competente". https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b6e c2. Accesso effettuato il 24 aprile 2017;

[42] L'articolo 12, paragrafo 3, del regolamento chiarisce le tempistiche per fornire queste informazioni.

[43] Il considerando 71 del regolamento afferma che:
"al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative

adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori, (...)".

[44] Considerando 71: "tale misura non dovrebbe riguardare un minore".

[45] Il parere 02/2013 del Gruppo di lavoro sulle applicazioni per dispositivi intelligenti (WP 202), adottato il 27 febbraio 2013, nella specifica sezione 3.10 dedicata ai minori, a pagina 26, specifica che "i titolari del trattamento del trattamento non dovrebbero trattare dati di minori, direttamente o indirettamente, a fini di pubblicità comportamentale, poiché è al di fuori della portata della comprensione di un minore e pertanto supera i limiti del trattamento lecito".

[46] Uno studio dell'UE sull'impatto del marketing attraverso i media sociali, i giochi online e le applicazioni mobili sul comportamento dei minori (in inglese) ha rilevato che le prassi di marketing hanno un impatto evidente sul comportamento dei minori. Tale studio era basato su minori di età compresa tra 6 e 12 anni.

[47] Un esempio di un codice di condotta che tratta di marketing nei confronti dei minori è quello prodotto da FEDMA, Codice di condotta - relazione, disponibile (in inglese) all'indirizzo: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. Accesso effettuato il 15 maggio 2017. Cfr. in particolare: "6.2 Gli operatori nel settore del marketing che si rivolgono ai minori e per i quali è probabile che i minori costituiscano una parte del loro pubblico, non dovrebbero sfruttare la credulità, la lealtà, vulnerabilità o la mancanza di esperienza dei minori.; 6.8.5 Gli operatori nel settore del marketing non dovrebbero condizionare l'accesso di un minore a un sito web alla raccolta di informazioni personali dettagliate. In particolare, incentivi speciali quali offerte di premi e giochi non dovrebbero essere usati per invogliare i minori a divulgare informazioni personali dettagliate".

[48] Come richiesto dall'articolo 5, paragrafo 2, del regolamento.

[49] Rispecchiando le prescrizioni di cui all'articolo 13, paragrafo 2, lettera f), all'articolo 14, paragrafo 2, lettera g), e all'articolo 22, paragrafo 3.

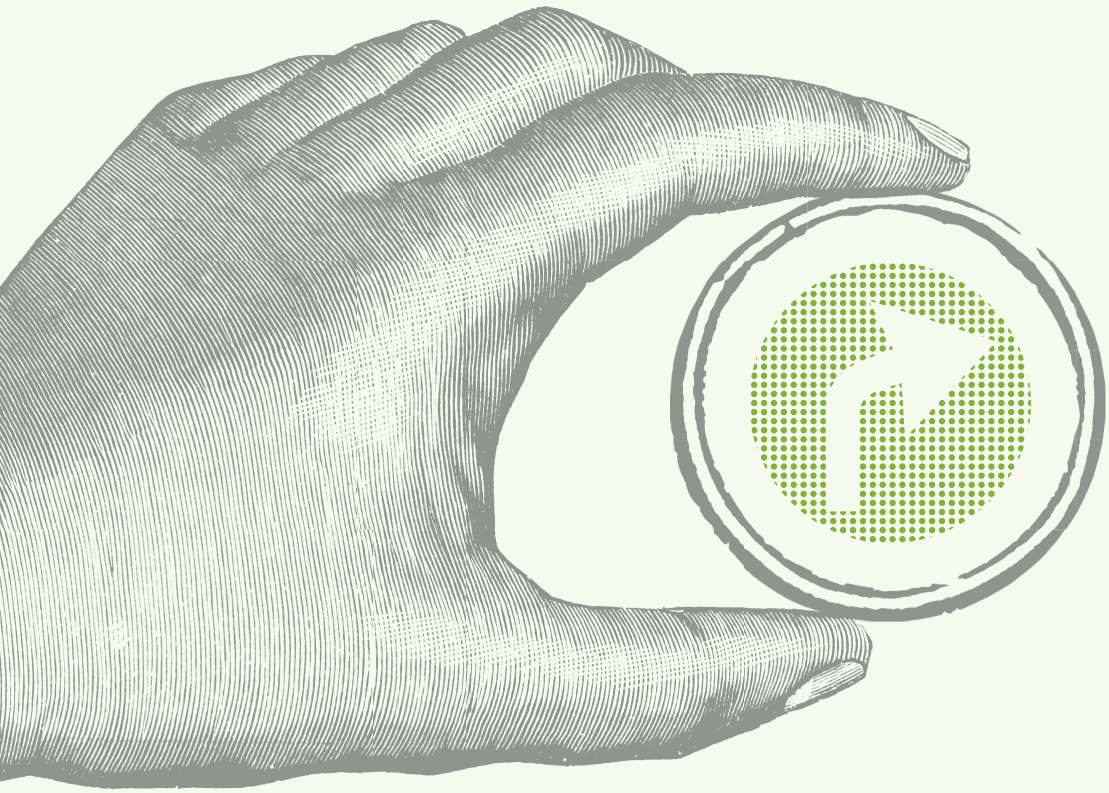
[50] Gruppo di lavoro articolo 29, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento 2016/679. 4 aprile 2017. https://www.garanteprivacy.it/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati. Accesso effettuato il 24 aprile 2017.

[51] Gruppo di lavoro articolo 29, Linee guida sui responsabili della protezione dei dati. 5 aprile 2017. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048. Accesso effettuato il 22 gennaio 2018.

[52] Il titolare del trattamento deve altresì assicurarsi di disporre di solide procedure destinate a garantire che può adempiere i suoi obblighi ai sensi degli articoli da 15 a 22 entro i termini previsti dal regolamento.

[53] Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection version 2.0 [Megadati, intelligenza artificiale, apprendimento automatico e protezione dei dati versione 2.0], 03/2017. Pagina 87, punto 194, marzo 2017. https://ico.org.uk/media/for - organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. Accesso effettuato il 24 aprile 2017.

2 Obblighi di titolari e responsabili - accountability



Premessa
Obblighi di titolari e responsabili - accountability

Il principio detto di "accountability", ossia di responsabilizzazione, è probabilmente la novità più rilevante del GDPR per quanto riguarda l'approccio complessivo alla gestione dei dati personali. In estrema sintesi, esso consiste nell'obbligo per il titolare o il responsabile del trattamento di garantire il rispetto delle norme sulla protezione dei dati attraverso strumenti e atti idonei a dimostrare tale rispetto. In questo senso, è soprattutto il Capo IV del GDPR a contenere gli elementi chiave di questo approccio responsabilizzante, alcuni dei quali (come si vedrà leggendo le linee-guida) non costituiscono una novità assoluta per chi si occupa di management o gestione del rischio in altri ambiti. Coerentemente con il principio di responsabilizzazione, il GDPR ha eliminato obblighi burocratici quali la notificazione preventiva dei trattamenti al Garante, sostituendovi l'obbligo per la quasi totalità di titolari e responsabili (con alcune eccezioni soprattutto per le piccole e medie imprese) di tenere un registro interno dei trattamenti. Questo registro è inteso come strumento fondamentale per garantire la conoscenza dei trattamenti in essere o previsti e individuarne gli elementi essenziali. Il WP29 ha ribadito tutto ciò nel "Position Paper" dedicato al registro dei trattamenti, chiarendo soprattutto gli ambiti molto ridotti dell'eccezione sopra ricordata.

Fra gli obblighi di sostanza che il GDPR ha esteso a tutti i titolari, e che finora si applicavano solo ai fornitori di servizi di comunicazione elettronica accessibili al pubblico in base alla direttiva e-privacy (2002/58/CE), vi è anche quello di notificare al Garante (e di comunicare, in certi casi, agli interessati) le violazioni di dati personali (o "data breach"). Il WP29 ha ritenuto necessario chiarire sia cosa rappresenti un data breach (attraverso una serie di esempi) sia in quali casi si realizzino le condizioni che rendono necessaria la notifica al Garante – poiché anche per il data breach si applica il principio di valutazione del rischio per i diritti e le libertà degli interessati conseguente alla violazione di sicurezza: la notifica al Garante non è dunque un adempimento automatico. Le linee-guida forniscono, infine, una griglia di indicazioni sui casi più rischiosi in questo ambito, nei quali è necessario comunicare

il data breach anche agli stessi interessati perché questi possano adottare le tutele più opportune.

Un'altra delle novità importanti del GDPR è rappresentata dall'obbligo, in determinati casi, di condurre una valutazione di impatto sulla protezione dei dati. Anche in questo caso si tratta di una delle espressioni primarie del principio di responsabilizzazione, perché una tale operazione serve a garantire che il titolare si preoccupi di minimizzare l'impatto di un trattamento (in termini di rischi per i diritti e le libertà delle persone) prima di procedere al trattamento stesso, tutte le volte in cui quest'ultimo, per le sue caratteristiche, comporti molto probabilmente un rischio "elevato". Nelle linee-guida in materia si chiariscono sia i criteri di rischio elevato dei quali tenere conto ai fini della valutazione di impatto, sia le modalità di conduzione della valutazione di impatto anche alla luce di standard internazionali in materia; si descrive, infine, un percorso che guida il titolare nel decidere se e come procedere a tale valutazione.

Analoghe le ragioni alla base delle linee-guida sui responsabili della protezione dati (RPD), cioè quelle figure che il GDPR ha introdotto (in alcuni casi in via obbligatoria, per esempio per i soggetti pubblici) per facilitare l'applicazione del GDPR stesso all'interno delle aziende o degli enti. Proprio la necessità di garantire la competenza, l'indipendenza e l'efficacia dell'azione di queste figure - che sono sostanzialmente nuove nel panorama italiano, ma note da tempo in altri Paesi - hanno spinto il WP29 a delineare un percorso sia per la selezione e il posizionamento corretti del RPD all'interno della struttura del titolare o del responsabile, sia per le attività che il RPD dovrà svolgere (sensibilizzazione interna, interfaccia con l'Autorità e gli interessati, ausilio del titolare o del responsabile in tutte le attività in cui si sostanzia la loro "accountability", a cominciare dalla valutazione di impatto). Il Garante ha, per parte sua, aggiunto a queste linee-guida alcune FAQ che gettano luce ulteriore sui criteri e gli obblighi di designazione di un RPD nei settori pubblico e privato e sui loro principali adempimenti.

Quale strumento atto a dimostrare il rispetto delle norme in materia di protezione dei dati, il GDPR ha introdotto la possibilità per i titolari di fare affidamento sulla certificazione di prodotti o servizi connessi al trattamento di dati personali, lasciando liberi i singoli Stati di decidere come organizzare il sistema nazionale di certificazione. Posto che la certificazione non rappresenta un obbligo, essendo frutto di una scelta volontaria e, in questo senso, pienamente rispondente al principio di responsabilizzazione, i Garanti europei hanno ritenuto necessario indicare criteri comuni per la certificazione, sia essa svolta direttamente dalle Autorità di protezione dati ovvero da organismi di certificazione, così da evitare una frammentazione eccessiva che sarebbe contraria alla volontà di generare un comune quadro europeo di garanzie attraverso il GDPR. In base a tali criteri dovranno quindi indirizzarsi sia le attività di certificazione vere e proprie, sia la messa a punto di nuovi schemi di certificazione, alla luce degli elementi giudicati imprescindibili al fine di garantire la compliance rispetto al GDPR. Fondamentale sarà, al riguardo, la chiara individuazione dell'oggetto della certificazione, che non potrà assumere contorni indi-

stinti o eccessivamente generici: difficilmente quindi si potrà certificare un intero sistema di gestione delle informazioni personali, a meno di descrivere in modo compiuto e distinto ogni singola componente di tale sistema.

Il meccanismo della certificazione prevede che quest'ultima sia rilasciata in ogni caso da soggetti "accreditati" da terze parti, e per questo il GDPR dedica due articoli (42, 43) alla definizione dei meccanismi di accreditamento, lasciando agli Stati membri la possibilità di stabilire la ripartizione delle competenze in materia – se debba cioè essere un organismo nazionale di accreditamento a norma del Regolamento (Ue) 765/2008 o l'Autorità nazionale di controllo, oppure entrambi, a rilasciare l'accreditamento di organismi di certificazione in materia di protezione dei dati. Le Linee-guida 4/2018 forniscono alcune importanti indicazioni interpretative, destinate a tutti gli attori coinvolti (Stati membri, Autorità di controllo, organismi di certificazione, titolari o responsabili del trattamento). In particolare, esse illustrano i termini-chiave del processo di accreditamento e chiariscono (con l'aiuto di un Allegato di prossima pubblicazione) i requisiti aggiuntivi che le Autorità di controllo dovranno approvare, come previsto dal GDPR, ai fini dell'accreditamento di organismi di certificazione nel settore della protezione dei dati. Tali requisiti dovranno essere identici a prescindere dal soggetto che effettua l'accreditamento - per garantire uniformità e affidabilità paneuropee - e dovranno focalizzarsi sulle caratteristiche di competenza (settoriale) e di indipendenza degli organismi di certificazione che desiderano accreditarsi.

Le deroghe all'obbligo di tenuta di un registro delle attività di trattamento previste dall'articolo 30, paragrafo 5, del RGPD (*)

Il Gruppo di lavoro "Articolo 29" ha analizzato l'obbligo di tenere un registro delle attività di trattamento cui sono assoggettati titolari e responsabili del trattamento ai sensi dell'articolo 30 del RGPD. Il presente documento delinea la posizione del Gruppo "Articolo 29" in merito alle deroghe previste a tale obbligo.

Il considerando 13 del RGPD afferma quanto segue:

"Per tener conto della specifica situazione delle micro, piccole e medie imprese, il presente regolamento prevede una deroga per le organizzazioni che hanno meno di 250 dipendenti per quanto riguarda la conservazione delle registrazioni."

L'art. 30, paragrafo 5, traduce operativamente il considerando 13, prevedendo che l'obbligo di tenere un registro delle attività di trattamento non sussiste nel caso di *"imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10."*

Appare necessario fornire alcuni chiarimenti interpretativi della disposizione di cui sopra, come segnala l'elevato numero di richieste rivolte negli ultimi mesi alle autorità di controllo nazionali da parte delle aziende.

La deroga prevista al paragrafo 5 dell'art. 30 non è da intendersi come assoluta. Essa non si applica con riguardo a tre tipologie di trattamento:

- trattamenti che possono presentare un rischio per i diritti e le libertà dell'interessato;
- trattamenti non occasionali;
- trattamenti di categorie particolari di dati o di dati personali relativi a condanne penali e a reati.

Il Gruppo di lavoro "Articolo 29" evidenzia come la formulazione letterale dell'art. 30, paragrafo 5, preveda chiaramente che le tre tipologie di trattamento cui non si applica la deroga in oggetto sono reciprocamente alternative ("o"), cosicché in presenza di qualsivoglia fra esse nasce l'obbligo di tenere un registro delle attività di trattamento.

(*) *NDR. Traduzione a cura dell'Ufficio del Garante per la protezione dei dati personali del testo non disponibile in lingua italiana.*

Ne consegue che un titolare o un responsabile il quale, pur avendo meno di 250 dipendenti, versi in una situazione tale per cui il trattamento svolto possa presentare un rischio (si noti, non un rischio elevato) per i diritti e le libertà dell'interessato, oppure tratti dati personali in via non occasionale, oppure tratti categorie particolari di dati ai sensi dell'art. 9, paragrafo 1, o dati relativi a condanne penali e a reati di cui all'art. 10, dovrà tenere un registro delle attività di trattamento.

Tuttavia, è sufficiente che questi soggetti tengano un registro delle attività di trattamento solo con riguardo alle tipologie di trattamento di cui all'art. 30, paragrafo 5.
Per esempio, una piccola azienda verosimilmente tratterà su base regolare dati relativi ai dipendenti. Ne deriva che un trattamento del genere non potrà essere ritenuto "occasionale" e dovrà quindi figurare nel registro delle attività di trattamento[1]. Viceversa, altri trattamenti che hanno realmente carattere "occasionale" non devono figurare nel registro delle attività di trattamento, purché non possano presentare un rischio per i diritti e le libertà degli interessati e non riguardino categorie particolari di dati o dati personali relativi a condanne penali e a reati.

Il Gruppo "Articolo 29" sottolinea che il registro delle attività di trattamento rappresenta uno strumento di grande utilità a supporto dell'analisi delle implicazioni di ogni trattamento, sia esso in corso o meno. Il registro facilita la valutazione concreta del rischio inerente le attività di trattamento svolte da un titolare o da un responsabile con riguardo ai diritti delle persone, nonché l'individuazione e la messa in atto di adeguate misure di sicurezza a tutela dei dati personali – tutti elementi essenziali del principio di responsabilizzazione sancito dal RGPD.

Per molte imprese di piccolissime, piccole o medie dimensioni, la tenuta di un registro delle attività di trattamento difficilmente rappresenterà un aggravio rilevante. Tuttavia, il Gruppo "Articolo 29" riconosce che le disposizioni dell'art. 30 configurano un nuovo adempimento amministrativo per titolari e responsabili e invita, pertanto, le autorità nazionali di controllo a supportare gli sforzi delle piccole e medie imprese attraverso la messa a disposizione di strumenti atti a facilitare la creazione e la gestione del registro in questione. Per esempio, l'autorità di controllo potrebbe pubblicare sul proprio sito web un modello semplificato utilizzabile dalle piccole e medie imprese per tenere il registro delle attività di trattamento che non ricadono nell'ambito della deroga di cui all'art. 30, paragrafo 5.

[1] Il Gruppo di lavoro "Articolo 29" ritiene che un trattamento sia da ritenersi "occasionale" se non viene condotto su base regolare e ha luogo al di fuori della normale attività imprenditoriale o di altro genere svolta dal titolare o dal responsabile. Si vedano le Linee-guida del Gruppo "Articolo 29" sull'art. 49 del Regolamento 2016/679 (WP262).

Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 [WP 250 rev. 01]

Adottate il 3 ottobre 2017
Versione emendata e adottata in data 6 febbraio 2018

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 della stessa,

visto il suo regolamento interno,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della Commissione europea, direzione generale Giustizia e consumatori, B -1049 Bruxelles, Belgio, ufficio MO-59 05/35.

Sito internet: //ec.europa.eu/justice/data-protection/index_en.htm

Indice

INTRODUZIONE

Il regolamento generale sulla protezione dei dati introduce l'obbligo di notificare una violazione dei dati personali (in appresso: "violazione") all'autorità di controllo[1] nazionale competente (oppure, in caso di violazione transfrontaliera, all'autorità capofila) e, in alcuni casi, di comunicare la violazione alle singole persone fisiche i cui dati personali sono stati interessati dalla violazione.

Attualmente l'obbligo di notifica delle violazioni esiste già per determinate organizzazioni, quali i fornitori di servizi di comunicazione elettronica accessibili al pubblico (come specificato nella direttiva 2009/136/CE e nel regolamento (UE) n. 611/2013)[2]. Inoltre, alcuni Stati membri dell'UE prevedono già un obbligo nazionale di notifica delle violazioni, che può consistere nell'obbligo di notificare violazioni che coinvolgono categorie di titolari del trattamento diversi dai fornitori di servizi di comunicazione elettronica accessibili al pubblico (ad esempio Germania e Italia) oppure nell'obbligo di segnalare tutte le violazioni riguardanti dati personali (ad esempio Paesi Bassi). Altri Stati membri dispongono di codici di buona pratica (ad esempio Irlanda[3]). Sebbene un certo numero di autorità di protezione dei dati dell'UE incoraggi già il titolare del trattamento a segnalare le violazioni, la direttiva 95/46/CE sulla protezione dei dati[4], che viene sostituita dal regolamento generale sulla protezione dei dati, non contiene uno obbligo specifico di notifica delle violazioni, pertanto tale obbligo sarà nuovo per numerose organizzazioni. Il regolamento generale sulla protezione dei dati rende ora la notifica obbligatoria per tutti i titolari del trattamento a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche[5]. Anche i responsabili del trattamento hanno un ruolo importante da svolgere e devono notificare qualsiasi violazione al proprio titolare del trattamento[6].

Il Gruppo di lavoro articolo 29 ("Gruppo di lavoro") ritiene che il nuovo obbligo di notifica presenti una serie di vantaggi. All'atto della notifica all'autorità di controllo, il titolare del trattamento può ottenere consulenza sull'eventuale necessità di informare le persone fisiche interessate. In effetti l'autorità di controllo può ordinare al titolare del trattamento di informare le persone fisiche interessate dalla violazione[7]. La comunicazione della violazione alle persone fisiche interessate consente al titolare del trattamento di fornire loro informazioni sui rischi derivanti dalla violazione e sui provvedimenti che esse possono prendere per proteggersi dalle potenziali conseguenze della violazione. Qualsiasi piano di risposta alle violazioni dovrebbe mirare a proteggere le persone fisiche e i loro dati personali. Di conseguenza, la notifica della violazione dovrebbe essere vista come uno strumento per migliorare la conformità in materia di protezione dei dati personali. Allo stesso tempo, va osservato che la mancata segnalazione di una violazione a una persona fisica o all'autorità di controllo può comportare l'imposizione di una sanzione al titolare del trattamento ai sensi dell'articolo 83.

I titolari e i responsabili del trattamento sono pertanto incoraggiati a pianificare anticipatamente e a mettere in atto processi per essere in grado di rilevare

e limitare tempestivamente gli effetti di una violazione, valutare il rischio per le persone fisiche[8] e stabilire se sia necessario notificare la violazione all'autorità di controllo competente e comunicarla alle persone fisiche interessate, ove necessario. La notifica all'autorità di controllo dovrebbe costituire parte del piano di intervento in caso di incidente.

Il regolamento contiene disposizioni che specificano quando e a chi la violazione deve essere notificata e quali informazioni devono essere fornite nel contesto della notifica. Le informazioni richieste per la notifica possono essere fornite procedendo per fasi, tuttavia il titolare del trattamento deve agire sempre in maniera tempestiva in caso di violazione.

Nel parere 03/2014 sulla notifica delle violazioni dei dati personali[9], il Gruppo di lavoro ha fornito orientamenti ai titolari del trattamento per aiutarli a decidere se effettuare la notifica agli interessati in caso di violazione. Il parere ha preso in considerazione l'obbligo dei fornitori di comunicazioni elettroniche ai sensi della direttiva 2002/58/CE e ha fornito esempi afferenti a più settori, nel contesto dell'allora progetto di regolamento generale sulla protezione dei dati, e ha illustrato le buone prassi per tutti i titolari del trattamento.

Le presenti linee guida spiegano gli obblighi di notifica e di comunicazione delle violazioni sanciti dal regolamento, nonché alcune misure che i titolari e i responsabili del trattamento possono intraprendere per soddisfare questi nuovi obblighi. Forniscono inoltre esempi di vari tipi di violazioni e i soggetti ai quali esse devono essere notificate nei diversi scenari.

I. NOTIFICA DELLE VIOLAZIONI DEI DATI PERSONALI AI SENSI DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

A. CONSIDERAZIONI DI BASE IN MATERIA DI SICUREZZA

Una delle prescrizioni del regolamento prevede che, mediante misure tecniche e organizzative adeguate, i dati personali siano trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali[10].
Di conseguenza, il regolamento impone tanto al titolare quanto al responsabile del trattamento di disporre di misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio cui sono esposti i dati personali trattati. Tali soggetti dovrebbero tenere conto: dello stato dell'arte e dei costi di attuazione; della natura, dell'oggetto, del contesto e delle finalità del trattamento; del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche[11]. Inoltre, il regolamento impone di mettere in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali, il che a sua volta consente di stabilire se scatta l'obbligo di notifica[12].

Di conseguenza, un aspetto fondamentale di qualsiasi politica di sicurezza dei dati è la capacità, ove possibile, di prevenire una violazione e, laddove essa si verifichi ciò nonostante, di reagire tempestivamente.

B. CHE COS'È UNA VIOLAZIONE DEI DATI PERSONALI?

1. DEFINIZIONE

Per poter porre rimedio a una violazione occorre innanzitutto che il titolare del trattamento sia in grado di riconoscerla. All'articolo 4, punto 12, il regolamento definisce la "violazione dei dati personali" come segue:

> "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Il significato di "distruzione" dei dati personali dovrebbe essere abbastanza chiaro: si ha distruzione dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento. Anche il concetto di "danno" dovrebbe essere relativamente evidente: si verifica un danno quando i dati personali sono stati modificati, corrotti o non sono più completi. Con "perdita" dei dati personali si dovrebbe invece intendere il caso in cui i dati potrebbero comunque esistere, ma il titolare del trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso. Infine, un trattamento non autorizzato o illecito può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure qualsiasi altra forma di trattamento in violazione del regolamento.

Esempio

Un esempio di perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati dei clienti del titolare del trattamento. Un altro esempio può essere il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un *ransomware* (*malware* del riscatto) oppure dal titolare del trattamento mediante una chiave non più in suo possesso.

Ciò che dovrebbe essere chiaro è che una violazione è un tipo di incidente di sicurezza. Tuttavia, come indicato all'articolo 4, punto 12, il regolamento si applica soltanto in caso di violazione di dati personali. La conseguenza di tale violazione è che il titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del regolamento. Questo punto mette in luce la differenza tra un incidente di sicurezza e una violazione dei dati personali: mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali[13].
I potenziali effetti negativi di una violazione sulle persone fisiche sono esaminati in appresso.

2. TIPI DI VIOLAZIONI DEI DATI PERSONALI

Nel parere 03/2014 sulla notifica delle violazioni, il Gruppo di lavoro ha spiegato che le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni[14]:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
- "violazione della disponibilità", in caso di perdita, accesso[15] o distruzione accidentali o non autorizzati di dati personali.

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.
Mentre stabilire se vi sia stata una violazione della riservatezza o dell'integrità è relativamente evidente, può essere meno ovvio determinare se vi è stata una violazione della disponibilità. Una violazione sarà sempre considerata una violazione della disponibilità se si è verificata una perdita o una distruzione permanente dei dati personali.

Esempio

Esempi di perdita di disponibilità possono aversi quando i dati vengono cancellati accidentalmente o da una persona non autorizzata, oppure, in caso di dati crittografati in maniera sicura, quando la chiave di decifratura viene persa. Se il titolare del trattamento non è in grado di ripristinare l'accesso ai dati, ad esempio ricorrendo a un backup, la perdita di disponibilità sarà considerata permanente.

Può verificarsi perdita di disponibilità anche in caso di interruzione significativa del servizio abituale di un'organizzazione, ad esempio un'interruzione di corrente o attacco da "blocco di servizio" (*denial of service*) che rende i dati personali indisponibili.

Ci si potrebbe chiedere se una perdita temporanea della disponibilità dei dati personali costituisca una violazione e, in tal caso, se si tratti di una violazione che richiede la notifica. L'articolo 32 del regolamento ("Sicurezza del trattamento") spiega che nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".
Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui

diritti e sulle libertà delle persone fisiche. Va precisato che l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "violazione della sicurezza" ai sensi dell'articolo 4, punto 12.

Come nel caso della perdita o distruzione permanente dei dati personali (o comunque di qualsiasi altro tipo di violazione), una violazione che implichi la perdita temporanea di disponibilità dovrebbe essere documentata in conformità all'articolo 33, paragrafo 5. Ciò aiuta il titolare del trattamento a dimostrare l'assunzione di responsabilità all'autorità di controllo, che potrebbe chiedere di consultare tali registrazioni[16]. Tuttavia, a seconda delle circostanze in cui si verifica, la violazione può richiedere o meno la notifica all'autorità di controllo e la comunicazione alle persone fisiche coinvolte. Il titolare del trattamento dovrà valutare la probabilità e la gravità dell'impatto dell'indisponibilità dei dati personali sui diritti e sulle libertà delle persone fisiche. Conformemente all'articolo 33, il titolare del trattamento dovrà effettuare la notifica a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Questo punto dovrà chiaramente essere valutato caso per caso.

Esempio

L'indisponibilità, anche solo temporanea, di dati medici critici di pazienti di un ospedale potrebbe presentare un rischio per i diritti e le libertà delle persone interessate, poiché, ad esempio, potrebbe comportare l'annullamento di operazioni e mettere a rischio le vite dei pazienti.

Viceversa, se i sistemi di una società di comunicazione non sono disponibili per diverse ore (ad esempio a causa di un'interruzione dell'alimentazione) e tale società non riesce a inviare newsletter ai propri abbonati è improbabile che ciò presenti un rischio per i diritti e le libertà delle persone fisiche.

Va notato che, sebbene una perdita di disponibilità dei sistemi del titolare del trattamento possa essere solo temporanea e non avere un impatto sulle persone fisiche, è importante che il titolare del trattamento consideri tutte le possibili conseguenze della violazione, poiché quest'ultima potrebbe comunque dover essere segnalata per altri motivi.

Esempio

Un'infezione da *ransomware* (software dannoso che cifra i dati del titolare del trattamento finché non viene pagato un riscatto) potrebbe comportare una perdita temporanea di disponibilità se i dati possono essere ripristinati da un backup. Tuttavia, si è comunque verificata un'intrusione nella rete e potrebbe essere richiesta una notifica se l'incidente è qualificato come violazione della riservatezza (ad esempio se chi ha effettuato l'attacco ha avuto accesso a dati personali) e ciò presenta un rischio per i diritti e le libertà delle persone fisiche.

3. POSSIBILI CONSEGUENZE DI UNA VIOLAZIONE DEI DATI PERSONALI

Una violazione può avere potenzialmente numerosi effetti negativi significativi sulle persone fisiche, che possono causare danni fisici, materiali o immateriali, ad esempio la perdita del controllo da parte degli interessati sui loro dati personali, la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale significativo alle persone fisiche interessate[17].

Di conseguenza, il regolamento impone al titolare del trattamento di notificare le violazioni all'autorità di controllo competente, fatta salva l'improbabilità che la violazione presenti il rischio che si verifichino detti effetti negativi. Laddove sia altamente probabile che tali effetti negativi si verifichino, il regolamento impone al titolare del trattamento di comunicare la violazione alle persone fisiche interessate non appena ciò sia ragionevolmente fattibile[18].

L'importanza di essere in grado di identificare una violazione, di valutare il rischio per le persone fisiche e, di conseguenza, di effettuare la notifica se necessario, è sottolineata nel considerando 87 del regolamento:

> "È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento".

Ulteriori linee guida sulla valutazione del rischio di effetti negativi per le persone fisiche sono considerate nella sezione IV.

Se il titolare del trattamento omette di notificare una violazione dei dati all'autorità di controllo o agli interessati oppure a entrambi, nonostante siano soddisfatte le prescrizioni di cui agli articoli 33 e/o 34, l'autorità di controllo dovrà effettuare una scelta e prendere in considerazione tutte le misure correttive a sua disposizione, tra cui l'imposizione di una sanzione amministrativa pecuniaria appropriata[19], in associazione a una misura correttiva ai sensi dell'articolo 58, paragrafo 2, oppure come sanzione indipendente. Qualora l'autorità opti per una sanzione amministrativa pecuniaria il suo valore può ammontare fino a un massimo di 10 000 000 EUR o fino al 2% del fatturato totale annuo globale di un'impresa ai sensi dell'articolo 83, paragrafo 4, lettera a), del regolamento. È altresì importante ricordare che, in alcuni casi, la mancata notifica di una violazione potrebbe rivelare l'assenza di misure di sicurezza o la loro inadeguatezza. Gli orientamenti del Gruppo di lavoro in materia di sanzioni

amministrative affermano che "qualora nell'ambito di un singolo caso siano state commesse congiuntamente più violazioni diverse, l'autorità di controllo può applicare le sanzioni amministrative pecuniarie a un livello che risulti effettivo, proporzionato e dissuasivo entro i limiti della violazione più grave". In tal caso, l'autorità di controllo avrà altresì la possibilità di comminare sanzioni per la mancata notifica o comunicazione della violazione (articoli 33 e 34), da un lato, e l'assenza di misure di sicurezza (adeguate) (articolo 32), dall'altro, in quanto si tratta di due infrazioni separate.

II. ARTICOLO 33 - NOTIFICA ALL'AUTORITÀ DI CONTROLLO

A. QUANDO EFFETTUARE LA NOTIFICA

1. PRESCRIZIONI DELL'ARTICOLO 33

L'articolo 33, paragrafo 1, stabilisce che:

> "In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo".

Il considerando 87[20] stabilisce che:

> "È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento".

2. QUANDO IL TITOLARE DEL TRATTAMENTO VIENE "A CONOSCENZA" DI UNA VIOLAZIONE?

Come indicato in precedenza, il regolamento impone al titolare del trattamento di notificare una violazione senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. Questo solleva la questione relativa al momento in cui il titolare del trattamento può considerarsi "a conoscenza" di una violazione. Il Gruppo di lavoro ritiene che il titolare del trattamento debba considerarsi "a conoscenza" nel momento in cui è ragione-

volmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali.

Tuttavia, come già osservato, il regolamento impone al titolare del trattamento di attuare tutte le misure tecniche e organizzative di protezione adeguate per stabilire immediatamente se si è verificata una violazione e informare tempestivamente l'autorità di controllo e gli interessati. Afferma altresì che è opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione e delle sue conseguenze e dei suoi effetti negativi per l'interessato[21]. Il titolare del trattamento è quindi tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva in modo da poter adottare le misure appropriate.

Il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione. In alcuni casi sarà relativamente evidente fin dall'inizio che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi. Tuttavia, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario.

Esempi

1. In caso di perdita di una chiave USB contenente dati personali non crittografati spesso non è possibile accertare se persone non autorizzate abbiano avuto accesso ai dati. Tuttavia, anche se il titolare del trattamento non è in grado di stabilire se si è verificata una violazione della riservatezza, tale caso deve essere notificato, in quanto sussiste una ragionevole certezza del fatto che si è verificata una violazione della disponibilità; il titolare del trattamento si considera venuto "a conoscenza" della violazione nel momento in cui si è accorto di aver perso la chiave USB.

2. Un terzo informa il titolare del trattamento di aver ricevuto accidentalmente i dati personali di uno dei suoi clienti e fornisce la prova della divulgazione non autorizzata. Dato che al titolare del trattamento è stata presentata una prova evidente di una violazione della riservatezza, non vi è dubbio che ne sia venuto "a conoscenza".

3. Un titolare del trattamento rileva che c'è stata una possibile intrusione nella sua rete. Controlla quindi i propri sistemi per stabilire se i dati personali ivi presenti sono stati compromessi e ne ottiene conferma. Ancora una volta, dato che il titolare del trattamento ha una chiara prova di una violazione non può esserci dubbio che sia venuto "a conoscenza" della stessa.

4. Un criminale informatico viola il sistema del titolare del trattamento e lo contatta per chiedere un riscatto. In tal caso, dopo aver verificato il suo sistema per accertarsi dell'attacco, il titolare del trattamento dispone di prove evidenti che si è verificata una violazione e non vi è dubbio che ne sia venuto a conoscenza.

Se una persona, un'organizzazione di comunicazione o un'altra fonte informa il titolare del trattamento di una potenziale violazione o se egli stesso rileva un incidente di sicurezza, il titolare del trattamento può effettuare una breve indagine per stabilire se la violazione si sia effettivamente verificata. Durante il periodo di indagine il titolare del trattamento non può essere considerato "a conoscenza". Tuttavia, si prevede che l'indagine iniziale inizi il più presto possibile e stabilisca con ragionevole certezza se si è verificata una violazione; può quindi seguire un'indagine più dettagliata.

Dopo che il titolare del trattamento è venuto a conoscenza di una violazione soggetta a notifica, la stessa deve essere notificata senza ingiustificato ritardo e, ove possibile, entro 72 ore. Durante questo periodo il titolare del trattamento dovrebbe valutare il rischio probabile per le persone fisiche al fine di stabilire se è soddisfatto il requisito per la notifica e quali siano le azioni necessarie per far fronte alla violazione. Tuttavia, il titolare del trattamento potrebbe già disporre di una valutazione iniziale del rischio potenziale che potrebbe derivare da una violazione come parte di una valutazione d'impatto sulla protezione dei dati[22] effettuata prima dello svolgimento del trattamento interessato. Tuttavia, tale valutazione può essere più generale rispetto alle circostanze specifiche di un'effettiva violazione e, pertanto, in ogni caso dovrà essere effettuata una valutazione aggiuntiva che tenga conto di tali circostanze. Per maggiori dettagli sulla valutazione del rischio, si rinvia alla sezione IV.

Nella maggior parte dei casi queste azioni preliminari dovrebbero essere completate subito dopo l'allerta iniziale (ossia quando il titolare o il responsabile del trattamento sospetta che si sia verificato un incidente di sicurezza che potrebbe interessare dati personali); dovrebbe richiedere più tempo soltanto in casi eccezionali.

Esempio

Una persona informa il titolare del trattamento di aver ricevuto un'e-mail da un soggetto che si fa passare per il titolare del trattamento, contenente dati personali relativi al suo (effettivo) utilizzo del servizio del titolare del trattamento, aspetto questo che suggerisce che la sicurezza del titolare del trattamento sia stata compromessa. Il titolare del trattamento conduce una breve indagine e individua un'intrusione nella propria rete e la prova di un accesso non autorizzato ai dati personali. Il titolare del trattamento si considera "a conoscenza" della violazione in questo momento e dovrà procedere alla notifica all'autorità di controllo a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Il titolare del trattamento dovrà prendere le opportune misure correttive per far fronte alla violazione.

Di conseguenza, il titolare del trattamento dovrebbe disporre di procedure interne per poter rilevare una violazione e porvi rimedio. Ad esempio, per rilevare talune irregolarità nel trattamento dei dati, il titolare o il responsabile del trattamento può utilizzare alcune misure tecniche certe come il flusso di dati e gli analizzatori di registri, dai quali è possibile definire eventi e allerte correlando qualsiasi dato di registro[23]. È importante che quando viene rilevata una violazione, la stessa venga segnalata al livello superiore appropriato di gestione, in maniera da poter essere trattata e, se del caso, notificata in conformità all'articolo 33 e, se necessario, all'articolo 34. Tali misure e meccanismi di segnalazione potrebbero essere dettagliati nei piani di intervento in caso di incidente del titolare del trattamento e/o nei dispositivi di governo societario. Ciò consentirà al titolare del trattamento di pianificare in maniera efficace e di stabilire chi ha la responsabilità operativa all'interno dell'organizzazione per la gestione di una violazione, nonché le modalità o l'opportunità di segnalare un incidente al livello gerarchico superiore, se del caso.

Il titolare del trattamento dovrebbe inoltre disporre di accordi con i responsabili del trattamento ai quali fa ricorso, i quali hanno a loro volta l'obbligo di notificare al titolare del trattamento eventuali violazioni (cfr. in appresso).

Sebbene spetti al titolare e al responsabile del trattamento mettere in atto misure adeguate per essere in grado di prevenire, reagire e affrontare una violazione, alcune misure pratiche dovrebbero essere prese in ogni caso:

- le informazioni relative a tutti gli eventi concernenti la sicurezza dovrebbero essere indirizzate a una persona responsabile o alle persone incaricate di gestire gli incidenti, stabilire l'esistenza di una violazione e valutare il rischio;
- il rischio per le persone fisiche a seguito di una violazione dovrebbe quindi essere valutato (probabilità di nessun rischio, di rischio o di rischio elevato) e le sezioni pertinenti dell'organizzazione dovrebbero esserne informate;
- se necessario si dovrebbe procedere alla notifica all'autorità di controllo ed eventualmente alla comunicazione della violazione alle persone fisiche interessate;
- allo stesso tempo, il titolare del trattamento dovrebbe agire in maniera tale da arginare la violazione e risolverla;
- la violazione dovrebbe essere documentata durante tutta la sua evoluzione.

Di conseguenza, dovrebbe essere chiaro che il titolare del trattamento è tenuto ad agire in relazione a qualsiasi allerta e stabilire se effettivamente si sia verificata una violazione. Tale breve periodo consente lo svolgimento di alcune indagini e dà al titolare del trattamento la possibilità di raccogliere prove e altre informazioni pertinenti. Tuttavia, dopo che il titolare del trattamento ha stabilito con ragionevole certezza che si è verificata una violazione, qualora siano soddisfatte le condizioni di cui all'articolo 33, paragrafo 1, è quindi necessario informare l'autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore[24]. Se il titolare del trattamento non agisce in maniera tempestiva

e risulta evidente che si è verificata una violazione, la sua inazione potrebbe essere considerata una mancata notifica ai sensi dell'articolo 33.
L'articolo 32 chiarisce che il titolare del trattamento e il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello adeguato di sicurezza dei dati personali: la capacità di individuare, trattare e segnalare tempestivamente una violazione deve essere considerata un aspetto essenziale di queste misure.

3. CONTITOLARI DEL TRATTAMENTO

L'articolo 26 riguarda i contitolari del trattamento e specifica che essi devono determinare le rispettive responsabilità in merito all'osservanza del regolamento[25]. Ciò includerà la determinazione di chi sarà responsabile di adempiere agli obblighi di cui agli articoli 33 e 34. Il Gruppo di lavoro raccomanda che gli accordi contrattuali tra i contitolari del trattamento includano disposizioni che stabiliscano quale titolare del trattamento assumerà il comando o sarà responsabile del rispetto degli obblighi di notifica delle violazioni previsti dal regolamento.

4. OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO

Sebbene il titolare del trattamento conservi la responsabilità generale per la protezione dei dati personali, il responsabile del trattamento svolge un ruolo importante nel consentire al titolare del trattamento di adempiere ai propri obblighi, segnatamente in materia di notifica delle violazioni. L'articolo 28, paragrafo 3, dispone che il trattamento da parte di un responsabile del trattamento è disciplinato da un contratto o da un altro atto giuridico, e precisa, alla lettera f), che il contratto o altro atto giuridico deve prevedere che il responsabile del trattamento "assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento".

L'articolo 33, paragrafo 2, chiarisce che se il titolare del trattamento ricorre a un responsabile del trattamento e quest'ultimo viene a conoscenza di una violazione dei dati personali che sta trattando per conto del titolare del trattamento, il responsabile del trattamento deve notificarla al titolare del trattamento "senza ingiustificato ritardo". Va notato che il responsabile del trattamento non deve valutare la probabilità di rischio derivante dalla violazione prima di notificarla al titolare del trattamento; spetta infatti a quest'ultimo effettuare la valutazione nel momento in cui viene a conoscenza della violazione. Il responsabile del trattamento deve soltanto stabilire se si è verificata una violazione e quindi notificarla al titolare del trattamento. Poiché quest'ultimo si serve del responsabile del trattamento per conseguire le proprie finalità, in linea di principio dovrebbe considerarsi "a conoscenza" della violazione non appena il responsabile del trattamento gliela notifica. L'obbligo del responsabile del trattamento di effettuare la notifica al titolare del trattamento consente a quest'ul-

timo di far fronte alla violazione e di stabilire se deve notificarla all'autorità di controllo ai sensi dell'articolo 33, paragrafo 1, e alle persone fisiche interessate ai sensi dell'articolo 34, paragrafo 1. Il titolare del trattamento potrebbe anche indagare sulla violazione, in quanto il responsabile del trattamento potrebbe non conoscere tutti i fatti pertinenti connessi alla violazione, ad esempio potrebbe ignorare se il titolare del trattamento detiene comunque una copia o un backup dei dati personali distrutti o persi. Tale circostanza può influire sull'eventualità che il titolare del trattamento debba effettuare la notifica.

Il regolamento non fissa un termine esplicito entro il quale il responsabile del trattamento deve avvertire il titolare del trattamento, salvo specificare che deve farlo "senza ingiustificato ritardo". Di conseguenza, il Gruppo di lavoro raccomanda al responsabile del trattamento di effettuare la notifica al titolare del trattamento tempestivamente, fornendo successivamente le eventuali ulteriori informazioni sulla violazione di cui venga a conoscenza. Ciò è importante al fine di aiutare il titolare del trattamento a soddisfare l'obbligo di notifica all'autorità di controllo entro 72 ore.

Come precedentemente spiegato, il contratto tra il titolare del trattamento e il responsabile del trattamento dovrebbe specificare le modalità per il soddisfacimento delle prescrizioni di cui all'articolo 33, paragrafo 2, e delle altre disposizioni del regolamento, tra cui i requisiti per la notifica tempestiva da parte del responsabile del trattamento, che serve per aiutare il titolare del trattamento a rispettare l'obbligo di segnalare la violazione all'autorità di controllo entro 72 ore.

Qualora fornisca servizi a più titolari del trattamento tutti interessati dal medesimo incidente, il responsabile del trattamento dovrà segnalare i dettagli dell'incidente a ciascun titolare del trattamento.
Il responsabile del trattamento può effettuare la notifica per conto del titolare del trattamento qualora quest'ultimo gli abbia concesso l'opportuna autorizzazione e ciò faccia parte degli accordi contrattuali tra il titolare del trattamento e il responsabile del trattamento. La notifica deve essere effettuata conformemente agli articoli 33 e 34. Tuttavia, è importante osservare che la responsabilità legale della notifica rimane in capo al titolare del trattamento.

B. FORNIRE INFORMAZIONI ALL'AUTORITÀ DI CONTROLLO

1. INFORMAZIONI DA FORNIRE

Quando il titolare del trattamento notifica una violazione all'autorità di controllo, l'articolo 33, paragrafo 3 stabilisce che la notifica deve almeno:

> "a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi".

Il regolamento non definisce le categorie di interessati né le registrazioni di dati personali. Tuttavia, il Gruppo di lavoro suggerisce che le categorie di interessati si riferiscono ai vari tipi di persone fisiche i cui dati personali sono stati oggetto di violazione: a seconda dei descrittori utilizzati, ciò potrebbe includere, tra gli altri, minori e altri gruppi vulnerabili, persone con disabilità, dipendenti o clienti. Analogamente, le categorie di registrazioni dei dati personali fanno riferimento ai diversi tipi di registrazioni che il titolare del trattamento può trattare, quali dati sanitari, registri didattici, informazioni sull'assistenza sociale, dettagli finanziari, numeri di conti bancari, numeri di passaporto, ecc.

Il considerando 85 chiarisce che uno degli scopi della notifica consiste nel limitare i danni alle persone fisiche. Di conseguenza, se i tipi di interessati o di dati personali rivelano un rischio di danno particolare a seguito di una violazione (ad esempio usurpazione d'identità, frode, perdite finanziarie, minaccia al segreto professionale) è importante che la notifica indichi tali categorie. In questo modo, l'obbligo di descrivere le categorie si collega all'obbligo di descriverne le probabili conseguenze della violazione.

Il fatto che non siano disponibili informazioni precise (ad esempio il numero esatto di interessati coinvolti) non dovrebbe costituire un ostacolo alla notifica tempestiva delle violazioni. Il regolamento consente di effettuare approssimazioni sul numero di persone fisiche interessate e di registrazioni dei dati personali coinvolte. Ci si dovrebbe preoccupare di far fronte agli effetti negativi della violazione piuttosto che di fornire cifre esatte. Di conseguenza, quando è evidente che c'è stata una violazione ma non se ne conosce ancora la portata, un modo sicuro per soddisfare gli obblighi di notifica è procedere a una notifica per fasi (cfr. in appresso).

L'articolo 33, paragrafo 3, stabilisce che nella notifica il titolare del trattamento "deve almeno" fornire le informazioni previste; di conseguenza il titolare del trattamento può, se necessario, fornire ulteriori informazioni. I diversi tipi di violazioni (riservatezza, integrità o disponibilità) possono richiedere la fornitura di ulteriori informazioni per spiegare in maniera esaustiva le circostanze di ciascun caso.

Esempio

Nell'ambito della notifica all'autorità di controllo, il titolare del trattamento può ritenere utile indicare il nome del responsabile del trattamento, qualora

quest'ultimo sia la causa di fondo della violazione, in particolare se quest'ultima ha provocato un incidente ai danni delle registrazioni dei dati personali di molti altri titolari del trattamento che fanno ricorso al medesimo responsabile del trattamento.

In ogni caso, l'autorità di controllo può richiedere ulteriori dettagli nel contesto dell'indagine su una violazione.

2. NOTIFICA PER FASI

A seconda della natura della violazione, il titolare del trattamento può avere la necessità di effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti relativi all'incidente. L'articolo 33, paragrafo 4, afferma pertanto:

"Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo".

Ciò significa che il regolamento prende atto del fatto che il titolare del trattamento non sempre dispone di tutte le informazioni necessarie su una violazione entro 72 ore dal momento in cui ne è venuto a conoscenza, dato che non sempre sono disponibili entro tale termine dettagli completi ed esaustivi su un incidente. Pertanto, il regolamento consente una notifica per fasi. È più probabile che ciò si verifichi in caso di violazioni più complesse, quali alcuni tipi di incidenti di sicurezza informatica nel contesto dei quali, ad esempio, può essere necessaria un'indagine forense approfondita per stabilire appieno la natura della violazione e la portata della compromissione dei dati personali. Di conseguenza, in molti casi il titolare del trattamento dovrà effettuare ulteriori indagini e dare seguito alla notifica fornendo informazioni supplementari in un secondo momento. Ciò è consentito a condizione che il titolare del trattamento indichi i motivi del ritardo, in conformità all'articolo 33, paragrafo 1. Il Gruppo di lavoro raccomanda che, all'atto della prima notifica all'autorità di controllo, il titolare del trattamento informi quest'ultima del fatto che non dispone ancora di tutte le informazioni richieste e che fornirà ulteriori dettagli in un momento successivo. L'autorità di controllo dovrebbe concordare le modalità e le tempistiche per la fornitura delle informazioni supplementari. Questo non impedisce al titolare del trattamento di trasmettere ulteriori informazioni in qualsiasi altro momento, qualora venga a conoscenza di ulteriori dettagli rilevanti sulla violazione che devono essere forniti all'autorità di controllo.

L'obiettivo dell'obbligo di notifica consiste nell'incoraggiare il titolare del trattamento ad agire prontamente in caso di violazione, a contenerla e, se possibile, a recuperare i dati personali compromessi e a chiedere un parere pertinente all'autorità di controllo. La notifica all'autorità di controllo entro le prime 72 ore può consentire al titolare del trattamento di assicurarsi che le decisioni in merito alla notifica o alla mancata notifica alle persone fisiche siano corrette.

Tuttavia, lo scopo della notifica all'autorità di controllo non è solo di ottenere orientamenti sull'opportunità di effettuare o meno la notifica alle persone fisiche interessate. In certi casi sarà evidente che, a causa della natura della violazione e della gravità del rischio, il titolare del trattamento dovrà effettuare la notifica alle persone fisiche coinvolte senza indugio. Ad esempio, se esiste una minaccia immediata di usurpazione d'identità oppure se categorie particolari di dati personali[26] vengono divulgate online, il titolare del trattamento deve agire senza ingiustificato ritardo per contenere la violazione e comunicarla alle persone fisiche coinvolte (cfr. sezione III). In circostanze eccezionali, ciò potrebbe persino aver luogo prima della notifica all'autorità di controllo. Più in generale, la notifica all'autorità di controllo non può fungere da giustificazione per la mancata comunicazione della violazione all'interessato laddove la comunicazione sia richiesta.

È opportuno inoltre precisare che se, dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione il titolare del trattamento può informarne l'autorità di controllo. Tali informazioni possono quindi essere aggiunte alle informazioni già fornite all'autorità di controllo e l'incidente può essere quindi registrato come un evento che non costituisce una violazione. Non si incorre in alcuna sanzione se si segnala un incidente che alla fine si rivela non essere una violazione.

Esempio

Un titolare del trattamento notifica all'autorità di controllo entro 72 ore l'individuazione di una violazione derivante dalla perdita di una chiave USB contenente una copia dei dati personali di alcuni dei suoi clienti. In seguito scopre che la chiave USB non era stata messa al suo posto e la recupera. Il titolare del trattamento aggiorna l'autorità di controllo e chiede la modifica della notifica.

Va osservato che un approccio per fasi alla notifica esiste già in forza degli obblighi di cui alla direttiva 2002/58/CE, del regolamento 611/2013 e nel quadro di altri incidenti segnalati di propria iniziativa.

3. NOTIFICHE EFFETTUATE IN RITARDO

L'articolo 33, paragrafo 1, chiarisce che, qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo deve essere corredata dei motivi del ritardo. Questa disposizione, unitamente al concetto di notifica in fasi, riconosce che il titolare del trattamento potrebbe non essere sempre in grado di notificare una violazione entro tale termine e che una notifica tardiva può essere consentita.

Tale scenario potrebbe aver luogo, ad esempio, qualora il titolare del trattamento subisca in poco tempo violazioni della riservatezza multiple e simili che coinvolgono allo stesso modo un gran numero di interessati. Il titolare del trattamento potrebbe prendere atto di una violazione e, nel momento in cui inizia l'indagi-

ne e prima della notifica, rilevare ulteriori violazioni analoghe, che hanno cause differenti. A seconda delle circostanze, il titolare del trattamento può impiegare del tempo per stabilire l'entità delle violazioni e, anziché notificare ciascuna violazione separatamente, effettuare una notifica significativa che rappresenta diverse violazioni molto simili tra loro, con possibili cause diverse. La notifica all'autorità di controllo potrebbe quindi aver luogo in ritardo, oltre le 72 ore dopo che il titolare del trattamento è venuto a conoscenza di tali violazioni.

A rigore di termini, ogni singola violazione costituisce un incidente segnalabile. Tuttavia, per evitare che il processo diventi eccessivamente oneroso, il titolare del trattamento può presentare una notifica "cumulativa" che rappresenta tutte le violazioni in questione, a condizione che riguardino il medesimo tipo di dati personali e che questi siano stati violati nel medesimo modo in un lasso di tempo relativamente breve. Se si verificano diverse violazioni riguardanti tipi diversi di dati personali, violati in maniere diverse, la notifica deve procedere secondo l'iter normale, segnalando ogni violazione conformemente all'articolo 33.

Sebbene il regolamento consenta di effettuare la notifica in ritardo, questa non dovrebbe essere vista come la regola. È opportuno sottolineare che le notifiche cumulative possono essere effettuate anche per più violazioni analoghe segnalate entro 72 ore.

C. VIOLAZIONI TRANSFRONTALIERE E VIOLAZIONI PRESSO STABILIMENTI NON UE

1. VIOLAZIONI TRANSFRONTALIERE

In caso di trattamento transfrontaliero[27] dei dati personali, una violazione può riguardare interessati in più Stati membri. L'articolo 33, paragrafo 1, chiarisce che quando si è verificata una violazione, il titolare del trattamento deve effettuare una notifica all'autorità di controllo competente ai sensi dell'articolo 55 del regolamento[28]. L'articolo 55, paragrafo 1, afferma che:

> "Ogni autorità di controllo è competente a eseguire i compiti assegnati e a esercitare i poteri a essa conferiti a norma del presente regolamento nel territorio del rispettivo Stato membro".

Tuttavia, l'articolo 56, paragrafo 1, stabilisce che:

> "Fatto salvo l'articolo 55, l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60".

Inoltre, l'articolo 56, paragrafo 6, afferma che:

> "L'autorità di controllo capofila è l'unico interlocutore del titolare del trattamento o del responsabile del trattamento in merito al trattamento transfrontaliero effettuato da tale titolare del trattamento o responsabile del trattamento".

Ciò significa che ogniqualvolta si verifichi una violazione nel contesto di un trattamento transfrontaliero e si renda necessaria la notifica, il titolare del trattamento dovrà effettuare la notifica all'autorità di controllo capofila[29]. Pertanto, nel redigere il proprio piano di risposta alle violazioni, il titolare del trattamento deve valutare quale autorità di controllo sia l'autorità capofila a cui indirizzare le notifiche[30]. Il titolare del trattamento sarà così in grado di rispondere tempestivamente alle violazioni e di adempiere i propri obblighi di cui all'articolo 33. Dovrebbe essere chiaro che, in caso di violazione che comporta un trattamento transfrontaliero, la notifica deve essere effettuata all'autorità di controllo capofila, che non si trova necessariamente nel luogo in cui si trovano gli interessati coinvolti o dove si è verificata la violazione. Al momento della notifica all'autorità capofila, il titolare del trattamento dovrebbe indicare, se del caso, se la violazione coinvolge stabilimenti situati in altri Stati membri e gli Stati membri in cu potrebbero esserci interessati colpiti dalla violazione. Se nutre dei dubbi sull'identità dell'autorità di controllo capofila, il titolare del trattamento deve come minimo effettuare la notifica all'autorità di controllo locale del luogo in cui si è verificata la violazione.

2. VIOLAZIONI PRESSO STABILIMENTI NON UE

L'articolo 3 definisce l'ambito di applicazione territoriale del regolamento, che si applica anche al trattamento di dati personali effettuato da un titolare del trattamento o un responsabile del trattamento che non è stabilito nell'UE. In particolare, l'articolo 3, paragrafo 2, afferma che[31]:

> "Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
>
> a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
>
> b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione".

Anche l'articolo 3, paragrafo 3, è pertinente al riguardo e afferma che[32]:

> "Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico".

Se un titolare del trattamento non stabilito nell'UE è soggetto all'articolo 3, pa-

ragrafo 2, oppure all'articolo 3, paragrafo 3, e constata una violazione, è quindi comunque vincolato agli obblighi di notifica di cui agli articoli 33 e 34. L'articolo 27 impone al titolare del trattamento (e al responsabile del trattamento) di designare un rappresentante nell'Unione europea nel caso in cui si applichi l'articolo 3, paragrafo 2. In tali casi, il Gruppo di lavoro raccomanda di inviare la notifica all'autorità di controllo dello Stato membro in cui è stabilito il rappresentante del titolare del trattamento nell'UE[33]. Analogamente, se un responsabile del trattamento è soggetto all'articolo 3, paragrafo 2, sarà tenuto a rispettare gli obblighi imposti ai responsabili del trattamento, in particolare l'obbligo di notificare una violazione al titolare del trattamento ai sensi dell'articolo 33, paragrafo 2.

D. CIRCOSTANZE NELLE QUALI NON È RICHIESTA LA NOTIFICA

L'articolo 33, paragrafo 1, chiarisce che se è "improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche" tale violazione non è soggetta a notifica all'autorità di controllo. Un esempio potrebbe essere quello di dati personali già disponibili pubblicamente, la cui divulgazione non costituirebbe un rischio probabile per la persona fisica. Questa esenzione dalla notifica è in contrasto con gli attuali obblighi di notifica delle violazioni imposti ai fornitori di servizi di comunicazione elettronica accessibili al pubblico di cui alla direttiva 2009/136/CE, che stabilisce che tutte le violazioni rilevanti devono essere notificate all'autorità competente.

Nel parere 03/2014 sulla notifica delle violazioni[34], il Gruppo di lavoro ha spiegato che una violazione della riservatezza di dati personali crittografati con un algoritmo all'avanguardia costituisce in ogni caso una violazione dei dati personali e deve essere notificata. Se però la riservatezza della chiave rimane intatta (ossia se la chiave non è stata compromessa nell'ambito di una violazione della sicurezza ed è stata generata in maniera tale da non poter essere individuata con i mezzi tecnici disponibili da qualcuno che non è autorizzato ad accedervi), in linea di principio i dati risultano incomprensibili. Di conseguenza è improbabile che la violazione possa influire negativamente sulle persone fisiche e quindi non dovrebbe essere loro comunicata[35]. Tuttavia, anche se i dati sono crittografati, una perdita o alterazione può avere effetti negativi per gli interessati ove il responsabile del trattamento non disponga delle necessarie copie di riserva. In tal caso, la notifica agli interessati dovrebbe essere necessaria anche se sono state adottate misure di protezione mediante crittografia.

Il Gruppo di lavoro ha altresì spiegato che lo stesso ragionamento si applica anche nel caso in cui dati personali, quali password, siano stati codificati in modo sicuro con un hash e un salt, il valore hash sia stato calcolato con una funzione di hash con chiave crittografica all'avanguardia, la chiave utilizzata per l'hashing dei dati non sia stata compromessa nell'ambito di una violazione della sicurezza e sia stata generata in maniera tale da non poter essere individuata con i mezzi tecnologici a disposizione di qualcuno che non è autorizzato ad accedervi.
Di conseguenza, se i dati personali sono stati resi sostanzialmente incompren-

sibili ai soggetti non autorizzati e se esiste una copia o un backup, una violazione della riservatezza che coinvolga dati personali correttamente crittografati potrebbe non dover essere notificata all'autorità di controllo, poiché è improbabile che tale violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche. Di conseguenza potrebbe non essere necessario nemmeno informare la persona interessata, dato che è improbabile che vi siano rischi elevati. Tuttavia, si dovrebbe tenere presente che, sebbene inizialmente la notifica possa non essere richiesta se non esiste un rischio probabile per i diritti e le libertà delle persone fisiche, la situazione può cambiare nel corso del tempo e il rischio dovrebbe essere rivalutato. Ad esempio, se la chiave risulta successivamente essere stata compromessa o essere stata esposta a una vulnerabilità nel software di cifratura, è possibile che sia ancora necessario procedere alla notifica.

Inoltre, va osservato che se si verifica una violazione in assenza di backup dei dati personali crittografati si è in presenza di una violazione della disponibilità che potrebbe presentare rischi per le persone fisiche e pertanto potrebbe richiedere la notifica. Analogamente, laddove si verifichi una violazione che implichi la perdita di dati crittografati, anche se esiste una copia di backup dei dati personali si potrebbe comunque trattare di una violazione soggetta a segnalazione, a seconda del periodo di tempo necessario per ripristinare i dati dal backup e dell'effetto che la mancanza di disponibilità ha sulle persone fisiche. Come afferma l'articolo 32, paragrafo 1, lettera c), un importante fattore di sicurezza è "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".

Esempio

Una violazione che non richiederebbe la notifica all'autorità di controllo sarebbe la perdita di un dispositivo mobile crittografato in maniera sicura, utilizzato dal titolare del trattamento e dal suo personale. Se la chiave di cifratura rimane in possesso del titolare del trattamento e non si tratta dell'unica copia dei dati personali, questi ultimi sarebbero inaccessibili a qualsiasi pirata informatico. Ciò significa che è improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati in questione. Se in seguito diventa evidente che la chiave di cifratura è stata compromessa o che il software o l'algoritmo di cifratura è vulnerabile, il rischio per i diritti e le libertà delle persone fisiche cambia e potrebbe quindi essere necessaria la notifica.

Tuttavia, si avrà mancato rispetto dell'articolo 33 se il titolare del trattamento non effettua la notifica all'autorità di controllo nel caso in cui i dati non siano stati effettivamente crittografati in maniera sicura. Di conseguenza, nel selezionare il software di cifratura, il titolare del trattamento deve valutare attentamente la qualità e la corretta attuazione della cifratura offerta, capire il livello di protezione effettivamente offerto e se quest'ultimo è appropriato in ragione dei rischi presentati. Il titolare del trattamento dovrebbe altresì avere familiarità con le specifiche modalità di funzionamento del prodotto di cifratura. Ad esempio, un dispositivo può essere crittografato una volta

spento, ma non mentre è in modalità stand-by. Alcuni prodotti che utilizzano la cifratura dispongono di "chiavi predefinite" che devono essere modificate da ciascun cliente per essere efficaci. La cifratura potrebbe essere considerata adeguata dagli esperti di sicurezza al momento della sua messa in atto, ma diventare obsoleta nel giro di pochi anni, il che significa che può essere messo in discussione il fatto che i dati siano sufficientemente crittografati dal prodotto in questione e che quest'ultimo fornisca un livello appropriato di protezione.

III. ARTICOLO 34 – COMUNICAZIONE ALL'INTERESSATO

A. INFORMARE L'INTERESSATO

In alcuni casi, oltre a effettuare la notifica all'autorità di controllo, il titolare del trattamento è tenuto a comunicare la violazione alle persone fisiche interessate.

L'articolo 34, paragrafo 1, afferma che:

> "Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo".

Il titolare del trattamento dovrebbe tenere a mente che la notifica all'autorità di controllo è obbligatoria a meno che sia improbabile che dalla violazione possano derivare rischi per i diritti e le libertà delle persone fisiche. Inoltre, laddove la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche occorre informare anche queste ultime. La soglia per la comunicazione delle violazioni alle persone fisiche è quindi più elevata rispetto a quella della notifica alle autorità di controllo, pertanto non tutte le violazioni dovranno essere comunicate agli interessati, il che li protegge da inutili disturbi arrecati dalla notifica.

Il regolamento afferma che la comunicazione di una violazione agli interessati dovrebbe avvenire "senza ingiustificato ritardo", il che significa il prima possibile. L'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi[36]. Come osservato in precedenza, a seconda della natura della violazione e del rischio presentato, la comunicazione tempestiva aiuterà le persone a prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

L'allegato B delle presenti linee guida fornisce un elenco non esaustivo di esempi di casi in cui una violazione può presentare un rischio elevato per le persone fisiche e, di conseguenza, in cui il titolare del trattamento deve comunicarla agli interessati.

B. INFORMAZIONI DA FORNIRE

Ai fini della comunicazione alle persone fisiche, l'articolo 34, paragrafo 2, specifica che:

> "La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d)".

Secondo tale disposizione, il titolare del trattamento deve fornire almeno le seguenti informazioni:

- una descrizione della natura della violazione;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Come esempio di misure adottate per far fronte alla violazione e attenuarne i possibili effetti negativi, il titolare del trattamento può dichiarare che, dopo aver notificato la violazione all'autorità di controllo pertinente, ha ricevuto consigli sulla gestione della violazione e sull'attenuazione del suo impatto. Se del caso, il titolare del trattamento dovrebbe anche fornire consulenza specifica alle persone fisiche sul modo in cui proteggersi dalle possibili conseguenze negative della violazione, ad esempio reimpostando le password in caso di compromissione delle credenziali di accesso. Ancora una volta, il titolare del trattamento può scegliere di fornire informazioni supplementari rispetto a quanto richiesto qui.

C. CONTATTARE L'INTERESSATO

In linea di principio, la violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato. In tal caso, si procede a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia (articolo 34, paragrafo 3, lettera c).

Nel comunicare una violazione agli interessati si devono utilizzare messaggi dedicati che non devono essere inviati insieme ad altre informazioni, quali aggiornamenti regolari, newsletter o messaggi standard. Ciò contribuisce a rendere la comunicazione della violazione chiara e trasparente.

Esempi di metodi trasparenti di comunicazione sono: la messaggistica diretta (ad esempio messaggi di posta elettronica, SMS, messaggio diretto), banner

o notifiche su siti web di primo piano, comunicazioni postali e pubblicità di rilievo sulla stampa. Una semplice comunicazione all'interno di un comunicato stampa o di un blog aziendale non costituirebbe un mezzo efficace per comunicare una violazione all'interessato. Il Gruppo di lavoro raccomanda al titolare del trattamento di scegliere un mezzo che massimizzi la possibilità di comunicare correttamente le informazioni a tutte le persone interessate. A seconda delle circostanze, ciò potrebbe significare che il titolare del trattamento dovrebbe utilizzare diversi metodi di comunicazione, anziché un singolo canale di contatto.

Inoltre il titolare del trattamento potrebbe dover garantire che la comunicazione sia accessibile in formati alternativi appropriati e lingue pertinenti al fine di assicurarsi che le persone fisiche siano in grado di comprendere le informazioni fornite loro. Ad esempio, nel comunicare una violazione a una persona, sarà di norma appropriata la lingua utilizzata durante il precedente normale corso degli scambi commerciali con il destinatario. Tuttavia, se la violazione riguarda interessati con i quali il titolare del trattamento non ha precedentemente interagito o, in particolare, interessati che risiedono in un altro Stato membro o in un altro paese non UE diverso da quello nel quale è stabilito il titolare del trattamento, la comunicazione nella lingua nazionale locale potrebbe essere accettabile, tenendo conto della risorsa richiesta. L'obiettivo principale è aiutare gli interessati a comprendere la natura della violazione e le misure che possono adottare per proteggersi.

Il titolare del trattamento è nella posizione migliore per stabilire il canale di contatto più appropriato per comunicare una violazione agli interessati, soprattutto se interagisce frequentemente con i suoi clienti. Tuttavia, è chiaro che il titolare del trattamento dovrebbe essere cauto nell'usare un canale di contatto compromesso dalla violazione, in quanto tale canale potrebbe essere utilizzato anche da autori di attacchi che si fanno passare per il titolare del trattamento.

Il considerando 86 spiega che:

> "Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione".

Il titolare del trattamento potrebbe quindi contattare e consultare l'autorità di controllo non soltanto per chiedere consiglio sull'opportunità di informare gli interessati in merito a una violazione ai sensi dell'articolo 34, ma anche sui messaggi appropriati da inviare loro e sul modo più opportuno per contattarli.

Parallelamente, il considerando 88 indica che la notifica di una violazione dovrebbe tenere "conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali". Ciò può significare che in determinate circostanze, ove giustificato e su consiglio delle autorità incaricate dell'applicazione della legge, il titolare del trattamento può ritardare la comunicazione della violazione agli interessati fino a quando la comunicazione non pregiudica più tale indagine. Tuttavia, passato tale arco di tempo, gli interessati dovrebbero comunque essere tempestivamente informati.

Se non ha la possibilità di comunicare una violazione all'interessato perché non dispone di dati sufficienti per contattarlo, il titolare del trattamento dovrebbe informarlo non appena sia ragionevolmente possibile farlo (ad esempio quando l'interessato esercita il proprio diritto ai sensi dell'articolo 15 di accedere ai dati personali e fornisce al titolare del trattamento le informazioni supplementari necessarie per essere contattato).

D. CIRCOSTANZE NELLE QUALI NON È RICHIESTA LA COMUNICAZIONE

L'articolo 34, paragrafo 3, stabilisce tre condizioni che, se soddisfatte, non richiedono la comunicazione agli interessati in caso di violazione, ossia:

- il titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi. Ciò potrebbe prevedere ad esempio la protezione dei dati personali con cifratura allo stato dell'arte oppure mediante tokenizzazione;
- immediatamente dopo una violazione, il titolare del trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche. Ad esempio, a seconda delle circostanze del caso, il titolare del trattamento può aver immediatamente individuato e intrapreso un'azione contro il soggetto che ha avuto accesso ai dati personali prima che questi fosse in grado di utilizzarli in qualsiasi modo. È necessario altresì tenere in debito conto delle possibili conseguenze di qualsiasi violazione della riservatezza, anche in questo caso, a seconda della natura dei dati in questione;
- contattare gli interessati richiederebbe uno sforzo sproporzionato[37], ad esempio nel caso in cui i dati di contatto siano stati persi a causa della violazione o non siano mai stati noti. Si pensi, ad esempio, al magazzino di un ufficio statistico che si è allagato e i documenti contenenti dati personali erano conservati soltanto in formato cartaceo. In tale circostanza il titolare del trattamento deve invece effettuare una comunicazione pubblica o prendere una misura analoga, tramite la quale gli interessati vengano informati in maniera altrettanto efficace. In caso di sforzo sproporzionato, si potrebbe altresì prevedere l'adozione di disposizioni tecniche per rendere le informazioni sulla violazione disponibili su richiesta, soluzione questa

che potrebbe rivelarsi utile per le persone fisiche che potrebbero essere interessate da una violazione ma che il titolare del trattamento non può altrimenti contattare.

Conformemente al principio di responsabilizzazione, il titolare del trattamento dovrebbe essere in grado di dimostrare all'autorità di controllo di soddisfare una o più di queste condizioni[38]. Va tenuto presente che, sebbene la comunicazione possa inizialmente non essere richiesta se non vi è alcun rischio per i diritti e le libertà delle persone fisiche, la situazione potrebbe cambiare nel corso del tempo e il rischio dovrebbe essere rivalutato.

Se il titolare del trattamento decide di non comunicare una violazione all'interessato, l'articolo 34, paragrafo 4, spiega che l'autorità di controllo può richiedere che lo faccia, qualora ritenga che la violazione possa presentare un rischio elevato per l'interessato. In alternativa, può ritenere che siano state soddisfatte le condizioni di cui all'articolo 34, paragrafo 3, nel qual caso la comunicazione all'interessato non è richiesta. Qualora stabilisca che la decisione di non effettuare la comunicazione all'interessato non sia fondata, l'autorità di controllo può prendere in considerazione l'esercizio dei poteri e delle sanzioni a sua disposizione.

IV. VALUTAZIONE DELL'ESISTENZA DI UN RISCHIO O DI UN RISCHIO ELEVATO

A. RISCHIO COME FATTORE CHE FA SCATTARE L'OBBLIGO DI NOTIFICA

Sebbene il regolamento introduca l'obbligo di notificare una violazione, non è obbligatorio farlo in tutte le circostanze:

- la notifica all'autorità di controllo competente è obbligatoria a meno che sia improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche;
- la comunicazione di una violazione alle persone fisiche diventa necessaria soltanto laddove la violazione possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Ciò significa che non appena il titolare del trattamento viene a conoscenza di una violazione, è fondamentale che non si limiti a contenere l'incidente, ma valuti anche il rischio che potrebbe derivarne. Questo per due motivi: innanzitutto conoscere la probabilità e la potenziale gravità dell'impatto sulle persone fisiche aiuterà il titolare del trattamento ad adottare misure efficaci per contenere e risolvere la violazione; in secondo luogo, ciò lo aiuterà a stabilire se è necessaria la notifica all'autorità di controllo e, se necessario, alle persone fisiche interessate.

Come spiegato in precedenza, la notifica di una violazione è obbligatoria a meno che sia improbabile che la violazione presenti un rischio per i diritti e le

libertà delle persone fisiche, mentre la comunicazione di una violazione agli interessati deve essere effettuata se è probabile che la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche. Tale rischio sussiste quando la violazione può comportare un danno fisico, materiale o immateriale per le persone fisiche i cui dati sono stati violati. Esempi di tali danni sono la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie e il pregiudizio alla reputazione. Il verificarsi di tale danno dovrebbe essere considerato probabile quando la violazione riguarda dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oppure che includono dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza[39].

B. FATTORI DA CONSIDERARE NELLA VALUTAZIONE DEL RISCHIO

I considerando 75 e 76 del regolamento suggeriscono che, di norma, nella valutazione del rischio si dovrebbero prendere in considerazione tanto la probabilità quanto la gravità del rischio per i diritti e le libertà degli interessati. Inoltre il regolamento afferma che il rischio dovrebbe essere valutato in base a una valutazione oggettiva.

Va osservato che la valutazione del rischio per i diritti e le libertà delle persone fisiche a seguito di una violazione esamina il rischio in maniera diversa rispetto alla valutazione d'impatto sulla protezione dei dati[40]. Quest'ultima considera tanto i rischi del trattamento dei dati svolto come pianificato, quanto quelli in caso di violazione. Nel considerare una potenziale violazione, esamina in termini generali la probabilità che la stessa si verifichi e il danno all'interessato che potrebbe derivarne; in altre parole, si tratta di una valutazione di un evento ipotetico. Nel caso di una violazione effettiva, l'evento si è già verificato, quindi l'attenzione si concentra esclusivamente sul rischio risultante dell'impatto di tale violazione sulle persone fisiche.

Esempio

Una valutazione d'impatto sulla protezione dei dati suggerisce che l'uso proposto di un determinato software di sicurezza per proteggere i dati personali costituisce una misura adeguata per garantire un livello di sicurezza adeguato al rischio che il trattamento presenterebbe altrimenti per le persone fisiche. Tuttavia, laddove una vulnerabilità diventi nota successivamente, ciò modifica l'idoneità del software a contenere il rischio per i dati personali protetti e richiede quindi una rivalutazione nel contesto di una valutazione d'impatto sulla protezione dei dati in corso.

Una vulnerabilità nel prodotto viene sfruttata in un secondo momento e si verifica una violazione. Il titolare del trattamento dovrebbe valutare le circostanze specifiche della violazione, i dati interessati e il potenziale livello di impatto sulle persone fisiche, nonché la probabilità che tale rischio si concretizzi.

Di conseguenza, nel valutare il rischio per le persone fisiche derivante da una violazione, il titolare del trattamento dovrebbe considerare le circostanze specifiche della violazione, inclusa la gravità dell'impatto potenziale e la probabilità che tale impatto si verifichi. Pertanto il Gruppo di lavoro raccomanda che la valutazione tenga conto dei seguenti criteri[41].

- Tipo di violazione

Il tipo di violazione verificatosi può influire sul livello di rischio presentato per le persone fisiche. Ad esempio, una violazione della riservatezza che ha portato alla divulgazione di informazioni mediche a soggetti non autorizzati può avere conseguenze diverse per una persona fisica rispetto a una violazione in cui i dettagli medici di una persona fisica sono stati persi e non sono più disponibili.

- Natura, carattere sensibile e volume dei dati personali

Ovviamente, un elemento fondamentale della valutazione del rischio sono il tipo e il carattere sensibile dei dati personali che sono stati compromessi dalla violazione. Solitamente più i dati sono sensibili, maggiore è il rischio di danni per le persone interessate; tuttavia si dovrebbero prendere in considerazione anche altri dati personali che potrebbero già essere disponibili sull'interessato. Ad esempio, è improbabile che la divulgazione del nome e dell'indirizzo di una persona fisica in circostanze ordinarie causi un danno sostanziale. Tuttavia, se il nome e l'indirizzo di un genitore adottivo sono divulgati a un genitore biologico, le conseguenze potrebbero essere molto gravi tanto per il genitore adottivo quanto per il bambino.

Violazioni relative a dati sulla salute, documenti di identità o dati finanziari come i dettagli di carte di credito, possono tutte causare danni di per sé, ma se tali dati fossero usati congiuntamente si potrebbe avere un'usurpazione d'identità. Di norma una combinazione di dati personali ha un carattere più sensibile rispetto a un singolo dato personale.

Alcuni tipi di dati personali possono sembrare relativamente innocui, tuttavia occorre valutare attentamente ciò che questi dati possono rivelare sull'interessato. Un elenco di clienti che accettano consegne regolari potrebbe non essere particolarmente sensibile, tuttavia gli stessi dati relativi a clienti che hanno richiesto l'interruzione delle loro consegne durante le vacanze potrebbero essere informazioni utili per dei criminali.

Analogamente, una piccola quantità di dati personali altamente sensibili può avere un impatto notevole su una persona fisica, mentre una vasta gamma di dettagli può rivelare molte più informazioni in merito alla stessa persona. Inoltre, una violazione che interessa grandi quantità di dati personali relative a molte persone può avere ripercussioni su un numero corrispondentemente elevato di persone.

- Facilità di identificazione delle persone fisiche

Un fattore importante da considerare è la facilità con cui un soggetto che può accedere a dati personali compromessi riesce a identificare persone specifiche o ad abbinare i dati con altre informazioni per identificare persone fisiche. A seconda delle circostanze, l'identificazione potrebbe essere possibile direttamente dai dati personali oggetto di violazione senza che sia necessaria alcuna ricerca speciale per scoprire l'identità dell'interessato, oppure potrebbe essere estremamente difficile abbinare i dati personali a una particolare persona fisica, ma sarebbe comunque possibile a determinate condizioni. L'identificazione può essere direttamente o indirettamente possibile a partire dai dati oggetto di violazione, tuttavia può dipendere anche dal contesto specifico della violazione e dalla disponibilità pubblica dei corrispondenti dettagli personali. Quest'ultima eventualità potrebbe essere più rilevante per le violazioni della riservatezza e della disponibilità.

Come indicato in precedenza, i dati personali protetti da un livello appropriato di cifratura saranno incomprensibili a persone non autorizzate che non dispongono della chiave di decifratura. Inoltre, anche una pseudonimizzazione opportunamente attuata (definita all'articolo 4, punto 5, come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile") può ridurre la probabilità che le persone fisiche vengano identificate in caso di violazione. Tuttavia, le tecniche di pseudonimizzazione da sole non possono essere considerate sufficienti a rendere i dati incomprensibili.

- Gravità delle conseguenze per le persone fisiche

A seconda della natura dei dati personali coinvolti in una violazione, ad esempio categorie particolari di dati, il danno potenziale alle persone che potrebbe derivarne può essere particolarmente grave soprattutto se la violazione può comportare furto o usurpazione di identità, danni fisici, disagio psicologico, umiliazione o danni alla reputazione. Se la violazione riguarda dati personali relativi a persone fisiche vulnerabili, queste ultime potrebbero essere esposte a un rischio maggiore di danni.

Il fatto che il titolare del trattamento sappia o meno che i dati personali sono nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose può incidere sul livello di rischio potenziale. Prendiamo una violazione della riservatezza nel cui ambito i dati personali vengono comunicati a un terzo di cui all'articolo 4, punto 10, o ad altri destinatari per errore. Una tale situazione può verificarsi, ad esempio, nel caso in cui i dati personali vengano inviati accidentalmente all'ufficio sbagliato di un'organizzazione o a un'organizzazione fornitrice utilizzata frequentemente. Il titolare del trattamento può chiedere al destinatario di restituire o distruggere in maniera sicura i dati ricevuti. In entrambi i casi, dato che il titolare del trattamento ha una relazione continuativa con tali soggetti e potrebbe essere a conoscenza delle loro pro-

cedure, della loro storia e di altri dettagli pertinenti, il destinatario può essere considerato "affidabile". In altre parole, il titolare del trattamento può ritenere che il destinatario goda di una certa affidabilità e può ragionevolmente aspettarsi che non leggerà o accederà ai dati inviati per errore e che rispetterà le istruzioni di restituirli. Anche se i dati fossero stati consultati, il titolare del trattamento potrebbe comunque confidare nel fatto che il destinatario non intraprenderà ulteriori azioni in merito agli stessi e restituirà tempestivamente i dati al titolare del trattamento e coopererà per garantirne il recupero. In tali casi, questo aspetto può essere preso in considerazione nella valutazione del rischio effettuata dal titolare del trattamento in seguito alla violazione; il fatto che il destinatario sia affidabile può neutralizzare la gravità delle conseguenze della violazione, anche se questo non significa che non si sia verificata una violazione. La probabilità che detta violazione presenti un rischio per le persone fisiche verrebbe però meno, quindi non sarebbe più necessaria la notifica all'autorità di controllo o alle persone fisiche interessate. Ancora una volta, tutto dipenderà dalle circostanze del caso concreto. Ciò nonostante il titolare del trattamento deve comunque conservare informazioni relative alla violazione nel contesto del suo dovere generale di conservare registrazioni in merito alle violazioni (cfr. seguente sezione V).

Si dovrebbe altresì tener conto della permanenza delle conseguenze per le persone fisiche laddove l'impatto possa essere considerato maggiore qualora gli effetti siano a lungo termine.

- Caratteristiche particolari dell'interessato

Una violazione può riguardare dati personali relativi a minori o ad altre persone fisiche vulnerabili, che possono di conseguenza essere soggette a un rischio più elevato di danno. Altri fattori concernenti la persona fisica potrebbero influire sul livello di impatto della violazione sulla stessa.

- Caratteristiche particolari del titolare del trattamento di dati

La natura e il ruolo del titolare del trattamento e delle sue attività possono influire sul livello di rischio per le persone fisiche in seguito a una violazione. Ad esempio, un'organizzazione medica tratterà categorie particolari di dati personali, il che significa che vi è una minaccia maggiore per le persone fisiche nel caso in cui i loro dati personali vengano violati, rispetto a una mailing list di un quotidiano.

- Numero di persone fisiche interessate

Una violazione può riguardare solo una o poche persone fisiche oppure diverse migliaia di persone fisiche, se non molte di più. Di norma, maggiore è il numero di persone fisiche interessate, maggiore è l'impatto che una violazione può avere. Tuttavia, una violazione può avere ripercussioni gravi anche su una sola persona fisica, a seconda della natura dei dati personali e del contesto nel quale i dati sono stati compromessi. Ancora una volta, l'aspetto fondamentale

consiste nel considerare la probabilità e la gravità dell'impatto sulle persone interessate.

- Aspetti generali

Pertanto, nel valutare il rischio che potrebbe derivare da una violazione, il titolare del trattamento dovrebbe considerare tanto la gravità dell'impatto potenziale sui diritti e sulle libertà delle persone fisiche e quanto la probabilità che tale impatto si verifichi. Chiaramente, se le conseguenze di una violazione sono più gravi, il rischio è più elevato; analogamente, se la probabilità che tali conseguenze si verifichino è maggiore, maggiore è anche il rischio. In caso di dubbio, il titolare del trattamento dovrebbe restare molto prudente ed effettuare la notifica. L'allegato B fornisce alcuni esempi utili di diversi tipi di violazioni che comportano rischi o rischi elevati per le persone fisiche.

L'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) ha elaborato raccomandazioni in merito a una metodologia di valutazione della gravità di una violazione, che possono essere utili per i titolari del trattamento e i responsabili del trattamento nella progettazione del loro piano di risposta per la gestione delle violazioni[42].

V. RESPONSABILIZZAZIONE E TENUTA DI REGISTRI

A. DOCUMENTARE LE VIOLAZIONI

Indipendentemente dal fatto che una violazione debba o meno essere notificata all'autorità di controllo, il titolare del trattamento deve conservare la documentazione di tutte le violazioni, come spiegato all'articolo 33, paragrafo 5:

> "Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo".

Tale obbligo è collegato al principio di responsabilizzazione, di cui all'articolo 5, paragrafo 2. Lo scopo della tenuta di registri delle violazioni non notificabili, oltre a quelle notificabili, è collegato anche agli obblighi del titolare del trattamento ai sensi dell'articolo 24, e l'autorità di controllo può richiedere di consultare tali registri. Di conseguenza il titolare del trattamento è incoraggiato a creare un registro interno delle violazioni, indipendentemente dal fatto che sia tenuto a effettuare la notifica o meno[43].

Sebbene spetti al titolare del trattamento determinare quale metodo e struttura utilizzare per documentare una violazione, determinate informazioni chiave dovrebbero essere sempre incluse. Come richiesto dall'articolo 33, paragrafo 5, il titolare del trattamento è tenuto a registrare i dettagli relativi alla violazione, comprese le cause, i fatti e i dati personali interessati. Dovrebbe

altresì indicare gli effetti e le conseguenze della violazione e i provvedimenti adottati per porvi rimedio.

Il regolamento non specifica un periodo di conservazione della documentazione. Nel caso in cui i registri contengano dati personali, spetterà al titolare del trattamento stabilire il periodo appropriato di conservazione in conformità ai principi connessi al trattamento dei dati personali[44] e soddisfare una base legittima per il trattamento[45]. Dovrà conservare la documentazione in conformità dell'articolo 33, paragrafo 5, nella misura in cui può essere chiamato a fornire prove all'autorità di controllo in merito al rispetto di tale articolo oppure, più in generale, del principio di responsabilizzazione. Ovviamente se i registri non contengono dati personali, il principio di limitazione della conservazione[46] previsto dal regolamento non si applica.

Oltre a queste informazioni, il Gruppo di lavoro raccomanda al titolare del trattamento di documentare anche il ragionamento alla base delle decisioni prese in risposta a una violazione. In particolare, se una violazione non viene notificata, è opportuno documentare una giustificazione di tale decisione. La giustificazione dovrebbe includere i motivi per cui il titolare del trattamento ritiene improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche[47]. In alternativa, se ritiene che una delle condizioni di cui all'articolo 34, paragrafo 3, sia soddisfatta, il titolare del trattamento dovrebbe essere in grado di fornire prove adeguate della circostanza che ricorre nel caso di specie.

Se il titolare del trattamento notifica una violazione all'autorità di controllo, ma la notifica avviene in ritardo, il titolare del trattamento deve essere in grado di fornire i motivi del ritardo; la documentazione relativa a tale circostanza potrebbe contribuire a dimostrare che il ritardo nella segnalazione è giustificato e non eccessivo.

Laddove comunichi una violazione alle persone fisiche interessate, il titolare del trattamento dovrebbe essere trasparente in merito alla violazione e comunicare in maniera efficace e tempestiva. Di conseguenza, conservando le prove di tale comunicazione il titolare del trattamento faciliterebbe la dimostrazione della propria assunzione di responsabilità e del proprio rispetto delle norme.

Per agevolare il rispetto degli articoli 33 e 34, sarebbe vantaggioso tanto per il titolare del trattamento quanto per il responsabile del trattamento disporre di una procedura di notifica documentata, che stabilisca la procedura da seguire una volta individuata una violazione, ivi compreso come contenere, gestire e porre rimedio all'incidente, valutare il rischio e notificare la violazione. A questo proposito, per dimostrare il rispetto del regolamento potrebbe anche essere utile dimostrare che i dipendenti sono stati informati dell'esistenza di tali procedure e meccanismi e che sanno come reagire alle violazioni.

Si noti che la mancata corretta documentazione di una violazione può comportare l'esercizio da parte dell'autorità di controllo dei suoi poteri ai sensi dell'ar-

ticolo 58 e l'imposizione di una sanzione amministrativa pecuniaria ai sensi dell'articolo 83.

B.RUOLO DEL RESPONSABILE DELLA PROTEZIONE DEI DATI

Il titolare del trattamento o il responsabile del trattamento può avere un responsabile della protezione dei dati[48], come richiesto dall'articolo 37 oppure su decisione volontaria come buona prassi. L'articolo 39 del regolamento stabilisce una serie di compiti obbligatori per il responsabile della protezione dei dati, ma non impedisce l'assegnazione di ulteriori compiti da parte del titolare del trattamento, se del caso.

Tra i compiti obbligatori del responsabile della protezione dei dati di particolare rilevanza per la notifica delle violazioni figurano quelli di fornire consulenza e informazioni al titolare del trattamento o al responsabile del trattamento, sorvegliare l'osservanza del regolamento e fornire un parere in merito alle valutazioni d'impatto sulla protezione dei dati. Il responsabile della protezione dei dati deve inoltre cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo e per gli interessati. Va inoltre osservato che, ai fini della notifica della violazione all'autorità di controllo, l'articolo 33, paragrafo 3, lettera b), impone al titolare del trattamento di fornire il nome e i dati di contatto del responsabile della protezione dei dati o di un altro punto di contatto.

Per quanto riguarda la documentazione delle violazioni, il titolare del trattamento o il responsabile del trattamento potrebbe chiedere il parere del proprio responsabile della protezione dei dati in merito alla struttura, all'impostazione e all'amministrazione della documentazione. Al responsabile della protezione dei dati potrebbe altresì essere affidato il compito di tenere i registri.

Questi compiti indicano che il responsabile della protezione dei dati dovrebbe svolgere un ruolo chiave nel fornire assistenza nella prevenzione delle violazioni o nella preparazione alle stesse, fornendo consulenza e monitorando il rispetto delle norme, nonché durante una violazione (ossia nel processo di notifica all'autorità di controllo) e durante qualsiasi successiva indagine da parte dell'autorità di controllo. In tale ottica, il Gruppo di lavoro raccomanda di informare tempestivamente il responsabile della protezione dei dati dell'esistenza di una violazione e di coinvolgerlo nella gestione delle violazioni e nel processo di notifica.

VI. Obblighi di notifica a norma di altri strumenti giuridici

Separatamente e in aggiunta alla notifica e alla comunicazione delle violazioni ai sensi del regolamento, il titolare del trattamento deve altresì essere a conoscenza di qualsiasi obbligo di notifica di incidenti di sicurezza previsto da altri atti legislativi associati cui potrebbe essere soggetto, e dell'eventuale obbligo parallelo di notificare all'autorità di controllo una violazione dei dati personali. Tali obblighi possono variare a seconda degli Stati membri. Esempi di obblighi

di notifica sanciti in altri strumenti giuridici e di modalità con cui si correlano con il regolamento generale sulla protezione dei dati sono i seguenti:

- Regolamento (UE) n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS)[49].

L'articolo 19, paragrafo 2, del regolamento eIDAS impone ai prestatori di servizi fiduciari di notificare all'organismo di vigilanza una violazione della sicurezza o la perdita di integrità che hanno un impatto significativo sul servizio fiduciario fornito o sui dati personali conservati in tale contesto. Ove applicabile, ossia quando tale violazione o perdita costituiscono altresì una violazione dei dati personali ai sensi del regolamento generale sulla protezione dei dati, il prestatore di servizi fiduciari deve effettuare la notifica anche all'autorità di controllo.

- Direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS)[50].

Gli articoli 14 e 16 della direttiva NIS impongono agli operatori di servizi essenziali e ai fornitori di servizi digitali di notificare gli incidenti di sicurezza alle loro autorità competenti. Come riconosciuto dal considerando 63 della direttiva NIS[51], gli incidenti di sicurezza possono spesso comportare una compromissione di dati personali. Sebbene la direttiva NIS imponga alle autorità competenti e alle autorità di controllo di cooperare e scambiare informazioni in tale contesto, rimane comunque il fatto che qualora tali incidenti siano o diventino violazioni di dati personali ai sensi del regolamento generale sulla protezione dei dati, tali operatori e/o fornitori sono tenuti a effettuare la notifica all'autorità di controllo in maniera distinta dagli obblighi di notifica degli incidenti a norma della direttiva NIS.

Esempio

Un fornitore di servizi cloud che notifica una violazione ai sensi della direttiva NIS può comunque essere tenuto a notificarla al titolare del trattamento se tale violazione include una violazione dei dati personali. Analogamente, un prestatore di servizi fiduciari che effettua una notifica a norma del regolamento eIDAS può anche essere tenuto a effettuare una notifica all'autorità competente per la protezione dei dati in caso di violazione.

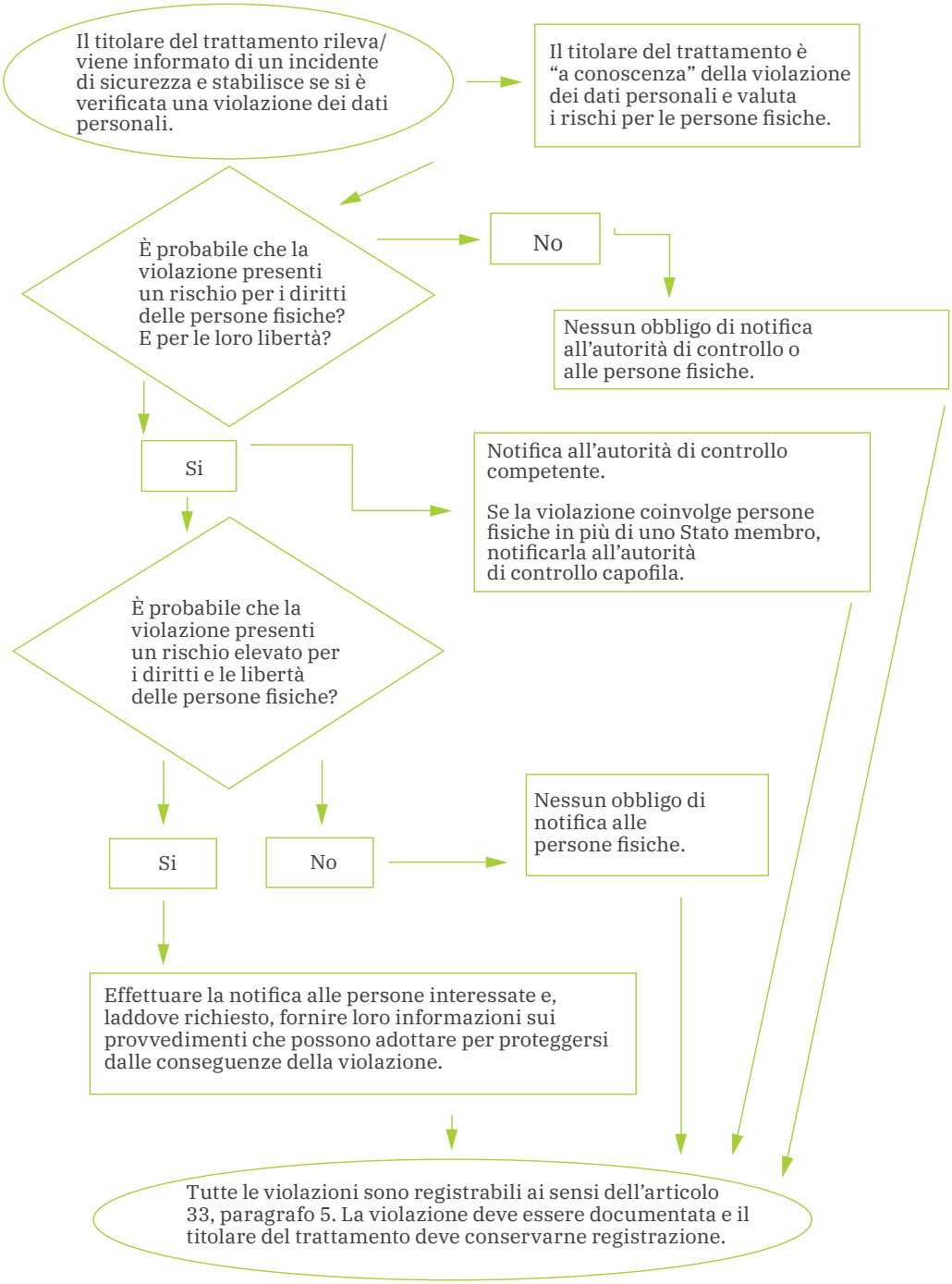
- Direttiva 2009/136/CE (direttiva sui diritti dei cittadini) e regolamento (UE) n. 611/2013 (regolamento sulla notifica delle violazioni).

I fornitori di servizi di comunicazione elettronica accessibili al pubblico nel contesto della direttiva 2002/58/CE[52] devono notificare le violazioni alle autorità nazionali competenti.

Il titolare del trattamento dovrebbe altresì essere a conoscenza di eventuali ulteriori obblighi di notifica in ambito giuridico, medico o professionale previsti da altri regimi applicabili.

VII. ALLEGATO

A. DIAGRAMMA DI FLUSSO CHE ILLUSTRA GLI OBBLIGHI DI NOTIFICA



B. ESEMPI DI VIOLAZIONI DEI DATI PERSONALI E DEI SOGGETTI A CUI NOTIFICARLE

I seguenti esempi non esaustivi aiuteranno il titolare del trattamento a stabilire se deve effettuare la notifica in diversi scenari di violazione dei dati personali. Questi esempi possono altresì contribuire a distinguere tra rischio e rischio elevato per i diritti e le libertà delle persone fisiche.

Esempio	Notifica all'autorità di controllo?	Comunicazione all'interessato?	Note/ raccomandazioni
I. Un titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	No.	No.	Fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.
II. Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico ai danni di tale servizio, i dati personali di persone fisiche vengono prelevati. Il titolare del trattamento ha clienti in un solo Stato membro.	Sì, segnalare l'evento all'autorità di controllo se vi sono probabili conseguenze per le persone fisiche.	Sì, segnalare l'evento alle persone fisiche a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per tali persone è elevata.	

III. Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento impedisce ai clienti di chiamare il titolare del trattamento e accedere alle proprie registrazioni.	No.	No.	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5. Il titolare del trattamento deve conservare adeguate registrazioni in merito.
IV. Un titolare del trattamento subisce un attacco tramite *ransomware* che provoca la cifratura di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, diventa evidente che l'unica funzionalità dal *ransomware* era la cifratura dei dati e che non vi erano altri *malware* presenti nel sistema.	Sì, effettuare la segnalazione all'autorità di controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità.	Sì, effettuare la segnalazione alle persone fisiche, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	Se fosse stato disponibile un backup e i dati avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione all'autorità di controllo o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora l'autorità di controllo fosse venuta a conoscenza dell'incidente con altri mezzi, avrebbe potuto prendere in considerazione lo svolgimento di un'indagine al fine di valutare il rispetto dei requisiti di sicurezza più ampi di cui all'articolo 32.

V. Una persona telefona al call center di una banca per segnalare una violazione dei dati. La persona ha ricevuto l'estratto conto mensile da un soggetto diverso. Il titolare del trattamento intraprende una breve indagine (ossia la conclude entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e che vi è una potenziale carenza sistemica che potrebbe comportare il coinvolgimento già occorso o potenziale di altre persone fisiche.	Sì.	La comunicazione va effettuata soltanto alle persone fisiche coinvolte in caso di rischio elevato e se è evidente che altre persone fisiche non sono state interessate dall'evento.	Se dopo ulteriori indagini si stabilisce che l'evento ha interessato un numero maggiore di persone fisiche è necessario comunicare questo sviluppo all'autorità di controllo, e il titolare del trattamento deve informarne le altre persone fisiche interessate se sussiste un rischio elevato per loro.
VI. Un titolare del trattamento gestisce un mercato online e ha clienti in più Stati membri. Tale mercato subisce un attacco informatico a seguito del quale i nomi utente, le password e la cronologia degli acquisti vengono pubblicati online dall'autore dell'attacco.	Sì, segnalare l'evento all'autorità di controllo capofila se la violazione riguarda un trattamento trans frontaliero.	Sì, dato che la violazione potrebbe comportare un rischio elevato.	Il titolare del trattamento dovrebbe prendere delle misure, ad esempio forzare il ripristino delle password degli account interessati, e altri provvedimenti per attenuare il rischio. Il titolare del trattamento dovrebbe altresì considerare qualsiasi altro obbligo di notifica, ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali.

VII. Una società di *hosting* di siti web che funge da responsabile del trattamento individua un errore nel codice che controlla l'autorizzazione dell'utente. A causa di tale vizio, qualsiasi utente può accedere ai dettagli dell'account di qualsiasi altro utente.	In veste di responsabile del trattamento, la società di *hosting* di siti web deve effettuare la notifica ai clienti interessati (i titolari del trattamento) senza ingiustificato ritardo. Supponendo che la società di *hosting* di siti web abbia condotto le proprie indagini, i titolari del trattamento interessati dovrebbero essere ragionevolmente certi di aver subito una violazione e pertanto è probabile che vengano considerati "a conoscenza" della violazione nel momento in cui hanno ricevuto la notifica da parte della società di *hosting* (il	Qualora non vi siano probabili rischi elevati per le persone fisiche non è necessario effettuare una comunicazione a tali persone.	La società di *hosting* di siti web (responsabile del trattamento) deve prendere in considerazione qualsiasi altro obbligo di notifica (ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali). Qualora non vi sia alcuna prova che tale vulnerabilità sia sfruttata presso uno dei suoi titolari del trattamento, la violazione potrebbe non essere soggetta all'obbligo di notifica, tuttavia potrebbe essere una violazione da registrare o essere il segno di un mancato rispetto dell'articolo 32.

	responsabile del trattamento). Il titolare del trattamento deve quindi effettuare la notifica all'autorità di controllo.		
VIII. Le cartelle cliniche di un ospedale sono indisponibili per un periodo di 30 ore a causa di un attacco informatico.	Sì, l'ospedale è tenuto a effettuare la notifica in quanto può verificarsi un rischio elevato per la salute e la tutela della vita privata dei pazienti.	Sì, informare le persone fisiche coinvolte.	
IX. I dati personali di un gran numero di studenti vengono inviati per errore a una mailing list sbagliata con più di 1000 destinatari.	Sì, segnalare l'evento all'autorità di controllo.	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	

X. Una e-mail di marketing diretto viene inviata ai destinatari nei campi “a:” o “cc:”, consentendo così a ciascun destinatario di vedere l’indirizzo e-mail di altri destinatari.	Sì, la notifica all’autorità di controllo può essere obbligatoria se è interessato un numero elevato di persone, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psico-terapeuta) o se altri fattori presentano rischi elevati (ad esempio, il messaggio di posta elettronica contiene le password iniziali).	Sì, segnalare l’evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato soltanto un numero limitato di indirizzi di posta elettronica.

NOTE

[1] Cfr. l'articolo 4, punto 21, del regolamento generale sulla protezione dei dati.

[2] Cfr. http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32009L0136 e http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32013R0611.

[3] Cfr. (in inglese) https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm.

[4] Cfr. http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:31995L0046.

[5] I diritti sanciti dalla Carta dei diritti fondamentali dell'Unione europea, disponibile all'indirizzo: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:12012P/TXT.

[6] Cfr. articolo 33, paragrafo 2. Questo concetto è analogo all'articolo 5 del regolamento (UE) n. 611/2013 nel quale si afferma che un fornitore incaricato di erogare una parte dei servizi di comunicazione elettronica (che non ha un legame contrattuale diretto con gli abbonati) è tenuto a notificare il fornitore che lo ha ingaggiato in caso di violazione di dati personali.

[7] Cfr. articolo 34, paragrafo 4 e articolo 58, paragrafo 2, lettera e).

[8] Ciò può essere garantito rispettando l'obbligo di monitoraggio e riesame previsto da una valutazione d'impatto sulla protezione dei dati, richiesta per i trattamenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche (articolo 35, paragrafi 1 e 11).

[9] Cfr. parere 03/2014 sulla notifica delle violazioni dei dati personali (in inglese) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

[10] Cfr. articolo 5, paragrafo 1, lettera f) e articolo 32.

[11] Articolo 32; cfr. anche considerando 83.

[12] Cfr. considerando 87.

[13] Va osservato che un incidente di sicurezza non si limita ai modelli di minacce nei quali un attacco viene effettuato ai danni di un'organizzazione dall'esterno della stessa, bensì include anche incidenti derivanti dal trattamento interno che violano i principi di sicurezza.

[14] Cfr. parere 03/2014.

[15] È un fatto assodato che "l'accesso" è una componente fondamentale della "disponibilità". Cfr. ad esempio il documento NIST SP800-53rev4, che definisce la "disponibilità" come la "garanzia di un accesso e un uso tempestivi e affidabili delle informazioni", disponibile (in inglese) all'indirizzo http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Anche il documento CNSSI-4009 fa riferimento a un "accesso tempestivo e affidabile ai dati e ai servizi dell'informazione per gli utenti autorizzati." Cfr. https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. Anche la norma ISO/IEC 27000:2016 definisce la "disponibilità" come la "proprietà di essere accessibile e utilizzabile su richiesta da un soggetto autorizzato": (in inglese) https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en.

[16] Cfr. articolo 33, paragrafo 5.

[17] Cfr. anche considerando 85 e 75.

[18] Cfr. anche il considerando 86.

[19] Per ulteriori dettagli, consultare le linee guida del Gruppo di lavoro riguardan-

ti l'applicazione e la previsione delle sanzioni amministrative pecuniarie disponibili qui: https://www.garanteprivacy.it/documents/10160/0/WP+253++Linee+guida+sanzioni+amministrative+pecuniarie+Reg+UE+2016+679.

[20] Anche il considerando 85 è importante in questo caso.

[21] Cfr. considerando 87.

[22] Cfr. le linee guida del Gruppo di lavoro in materia di valutazioni d'impatto sulla protezione dei dati qui: https://www.garanteprivacy.it/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati.

[23] Va osservato che anche i dati di registro che facilitano la verificabilità, ad esempio, della memorizzazione, delle modifiche o della cancellazione dei dati possono essere considerati dati personali relativi alla persona che ha avviato il trattamento corrispondente.

[24] Cfr. il regolamento (CEE, Euratom) n. 1182/71 che stabilisce le norme applicabili ai periodi di tempo, alle date e ai termini, disponibile all'indirizzo: http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:31971R1182&from=IT.

[25] Cfr. anche il considerando 79.

[26] Cfr. articolo 9.

[27] Cfr. articolo 4, paragrafo 23.

[28] Cfr. anche il considerando 122.

[29] Cfr. linee guida del Gruppo di lavoro per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento, disponibile (in inglese) all'indirizzo http://ec.europa.eu/newsroom/document.cfm?-doc_id=44102.

[30] Un elenco dei dati di contatto per tutte le autorità nazionali europee per la protezione dei dati è disponibile (in inglese) all'indirizzo: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm.

[31] Cfr. anche considerando 23 e 24.

[32] Cfr. anche il considerando 25.

[33] Cfr. considerando 80 e articolo 27.

[34] Gruppo di lavoro, Parere 03/2014 sulla notifica delle violazioni, (in inglese): http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

[35] Cfr. anche articolo 4, paragrafi 1 e 2, del regolamento 611/2013.

[36] Cfr. anche il considerando 86.

[37] Cfr. linee guida del Gruppo di lavoro sulla trasparenza, che prendono in considerazione la questione dello sforzo sproporzionato, disponibile (in inglese) all'indirizzo http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850.

[38] Cfr. articolo 5, paragrafo 2.

[39] Cfr. considerando 75 e 85.

[40] Cfr. le linee guida del Gruppo di lavoro in materia di valutazioni d'impatto sulla protezione dei dati qui: https://www.garanteprivacy.it/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati.

[41] L'articolo 3, paragrafo 2, del regolamento 611/2013 fornisce orientamenti sui fattori che dovrebbero essere presi in considerazione in relazione alla notifica di violazioni nel settore dei servizi di comunicazione elettronica che possono essere utili nel contesto della notifica ai sensi del regolamento generale sulla protezione dei dati. Cfr. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:it:PDF.

[42] ENISA, *Recommendations for a methodology of the assessment of severity of personal data breaches* [Raccomanda-

zioni in merito a una metodologia di valutazione della gravità delle violazioni dei dati personali], (disponibile in inglese) https://www.enisa.europa.eu/publications/dbn-severity.

[43] Il titolare del trattamento può scegliere di documentare le violazioni nel contesto del suo registro delle attività di trattamento che è mantenuto ai sensi dell'articolo 30. Non è richiesto un registro separato, a condizione che le informazioni rilevanti per la violazione siano chiaramente identificabili come tali e possano essere estratte su richiesta.

[44] Cfr. articolo 5.

[45] Cfr. articolo 6 e anche articolo 9.

[46] Cfr. articolo 5, paragrafo 1, lettera e).

[47] Cfr. considerando 85.

[48] Cfr. le linee guida del Gruppo di lavoro sui responsabili della protezione dei dati qui: https://www.garanteprivacy.it/documents/10160/0/WP+243+-+Linee-guida+-sui+responsabili+della+protezione+dei+dati+%28RPD%29.pdf.

[49] Cfr. http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ITA.

[50] Cfr. http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ITA.

[51] Considerando 63: **"***In molti casi gli incidenti compromettono dati personali. Al riguardo è opportuno che le autorità competenti e le autorità responsabili della protezione dei dati collaborino e si scambino informazioni su tutti gli aspetti pertinenti per affrontare le violazioni ai dati personali determinate dagli incidenti".*

[52] Il 10 gennaio 2017, la Commissione europea ha proposto un direttiva relativa alla vita privata e alle comunicazioni elettroniche che sostituirà la direttiva 2009/136/CE e sopprimerà gli obblighi di notifica. Tuttavia, fino a quando tale proposta non sarà approvata dal Parlamento europeo, l'attuale obbligo di notifica rimane in vigore, cfr. https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 [WP 248 rev. 01]

Adottate il 4 aprile 2017
come modificate e adottate da ultimo il 4 ottobre 2017

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 della stessa,

visto il suo regolamento interno,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e cittadinanza dell'Unione) della Commissione europea, direzione generale Giustizia, B -1049 Bruxelles, Belgio, ufficio MO-59 02/13.

Sito web: http://ec.europa.eu/justice/data-protection/index_en.htm

Indice

I. INTRODUZIONE

Il regolamento (UE) 2016/679[1] ("regolamento generale sulla protezione dei dati") si applicherà a partire dal 25 maggio 2018. L'articolo 35 del regolamento generale sulla protezione dei dati introduce il concetto di valutazione d'impatto sulla protezione dei dati[2], così come previsto anche dalla direttiva 2016/680[3].

Una valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali[4], valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento (cfr. anche l'articolo 24)[5]. In altre parole, **una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità.**

A norma del regolamento generale sulla protezione dei dati, l'inosservanza dei requisiti stabiliti per la valutazione d'impatto sulla protezione dei dati può portare a sanzioni pecuniarie imposte dall'autorità di controllo competente. La mancata esecuzione di una valutazione d'impatto sulla protezione dei dati nei casi in cui il trattamento è soggetto alla stessa (articolo 35, paragrafi 1, 3 e 4), l'esecuzione in maniera errata di detta valutazione (articolo 35, paragrafi 2 e da 7 a 9) oppure la mancata consultazione dell'autorità di controllo laddove richiesto (articolo 36, paragrafo 3, lettera e)), possono comportare una sanzione amministrativa pecuniaria pari a un importo massimo di 10 milioni di EUR oppure, nel caso di un'impresa, pari a fino al 2% del fatturato annuo globale dell'anno precedente, a seconda di quale dei due importi sia quello superiore.

II. CAMPO DI APPLICAZIONE DELLE PRESENTI LINEE GUIDA

Le presenti linee guida tengono conto dei seguenti documenti:

- dichiarazione del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN WP 218[6];
- linee guida sui responsabili della protezione dei dati del WP29 - 16/EN WP 243[7];
- parere del WP29 sulla limitazione della finalità - 13/EN WP 203[8];
- norme internazionali[9].

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento. Infatti, è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando il trattamento *"può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"*

(articolo 35, paragrafo 1). Al fine di assicurare un'interpretazione coerente delle circostanze in cui è obbligatorio realizzare una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 3), le presenti linee guida mirano innanzitutto a chiarire tale nozione e a fornire criteri per gli elenchi che devono essere adottati dalle autorità di protezione dei dati ai sensi dell'articolo 35, paragrafo 4.

A norma dell'articolo 70, paragrafo 1, lettera e), il comitato europeo per la protezione dei dati potrà pubblicare linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del regolamento generale sulla protezione dei dati. Lo scopo del presente documento è quindi quello di anticipare i futuri lavori del comitato europeo per la protezione dei dati e, di conseguenza, di chiarire le pertinenti disposizioni del regolamento generale sulla protezione dei dati in maniera da assistere i titolari del trattamento nel rispettare la legge, nonché da fornire la certezza del diritto a quei titolari del trattamento che sono tenuti a realizzare una valutazione d'impatto sulla protezione dei dati.

Le presenti linee guida mirano altresì a promuovere la redazione di:

- un elenco comune dell'Unione europea delle tipologie di trattamento per le quali è obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 4);
- un elenco comune dell'Unione europea delle tipologie di trattamento per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5);
- criteri comuni sulla metodologia per la realizzazione di una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5);
- criteri comuni che specifichino quando è necessario consultare l'autorità di controllo (articolo 36, paragrafo 1);
- raccomandazioni, ove possibile, basate sull'esperienza acquisita negli Stati membri dell'UE.

III. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI: SPIEGAZIONE DEL REGOLAMENTO

Il regolamento generale sulla protezione dei dati prevede che i titolari del trattamento attuino misure adeguate per garantire ed essere in grado di dimostrare il rispetto di detto regolamento, tenendo conto tra l'altro dei "rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" (articolo 24, paragrafo 1). L'obbligo per i titolari del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati va inteso nel contesto dell'obbligo generale, cui gli stessi sono soggetti, di gestire adeguatamente i rischi[10] presentati dal trattamento di dati personali.

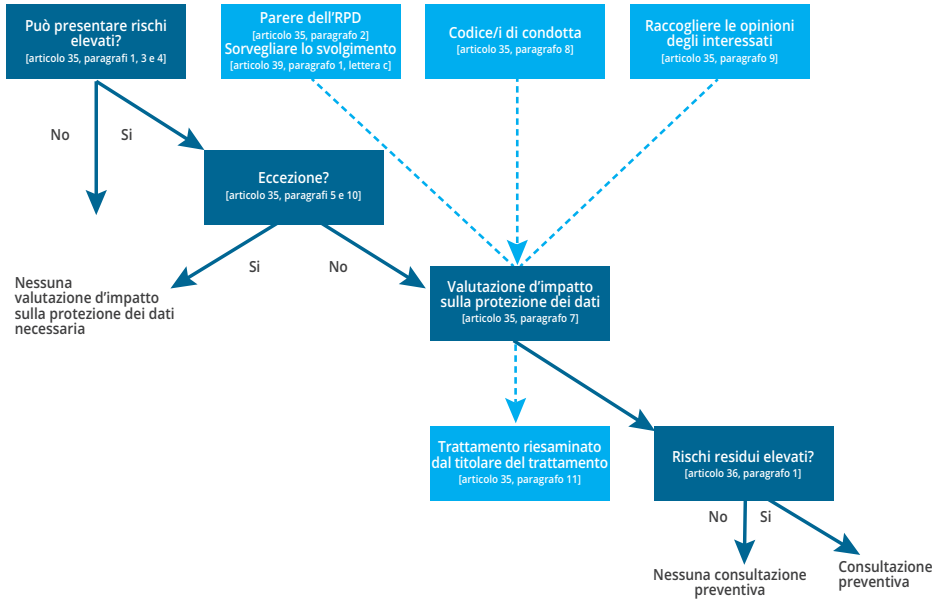
Un "rischio" è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. La "gestione dei rischi", invece, può

essere definita come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.

L'articolo 35 fa riferimento al possibile rischio elevato "per i diritti e le libertà delle persone fisiche". Come indicato nella dichiarazione del gruppo di lavoro articolo 29 sulla protezione dei dati sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati, il riferimento a "diritti e libertà" degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento. Al contrario, è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1). Il semplice fatto che le condizioni che comportano l'obbligo di realizzare una valutazione d'impatto sulla protezione dei dati non siano soddisfatte non diminuisce tuttavia l'obbligo generale, cui i titolari del trattamento sono soggetti, di attuare misure volte a gestire adeguatamente i rischi per i diritti e le libertà degli interessati. In pratica, ciò significa che i titolari del trattamento devono continuamente valutare i rischi creati dalle loro attività al fine di stabilire quando una tipologia di trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche".

La figura che segue illustra i principi fondamentali relativi alla valutazione d'impatto sulla protezione dei dati di cui al regolamento generale sulla protezione dei dati:



A. CHE COSA ESAMINA UNA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI? UN SINGOLO TRATTAMENTO O UN INSIEME DI TRATTAMENTI SIMILI.

Una valutazione d'impatto sulla protezione dei dati può riguardare una singola operazione di trattamento dei dati. Tuttavia, l'articolo 35, paragrafo 1, indica che *"[u]na singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi"*. Il considerando 92 aggiunge che *"[v]i sono circostanze in cui può essere ragionevole ed economico effettuare una valutazione d'impatto sulla protezione dei dati che verta su un oggetto più ampio di un unico progetto, per esempio quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi titolari del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata"*.

Si potrebbe ricorrere a una singola valutazione d'impatto sulla protezione dei dati nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. In effetti, le valutazioni d'impatto sulla protezione dei dati mirano a studiare sistematicamente nuove situazioni che potrebbero portare a rischi elevati per i diritti e le libertà delle persone fisiche e non è necessario realizzare una valutazione d'impatto sulla protezione dei dati nei casi (ad esempio operazioni di trattamento in un contesto specifico e per una finalità specifica) che sono già stati studiati. Questo potrebbe essere il caso in cui si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità. Ad esempio, un gruppo di autorità comunali che istituiscono ciascuna un sistema di televisione a circuito chiuso simile potrebbe svolgere una singola valutazione d'impatto sulla protezione dei dati che copra il trattamento svolto da tali titolari del trattamento distinti; oppure un gestore ferroviario (un titolare del trattamento unico) potrebbe esaminare la videosorveglianza in tutte le sue stazioni ferroviarie realizzando una singola valutazione d'impatto sulla protezione dei dati. Ciò può essere applicabile anche a trattamenti simili attuati da vari titolari del trattamento di dati. In questi casi, è necessario condividere o rendere pubblicamente accessibile una valutazione d'impatto sulla protezione dei dati di riferimento, attuare le misure descritte nella stessa, e fornire una giustificazione per la realizzazione di una singola valutazione d'impatto sulla protezione dei dati.

Qualora il trattamento coinvolga contitolari del trattamento, questi ultimi devono definire con precisione le rispettive competenze. La loro valutazione d'impatto sulla protezione dei dati deve stabilire quale parte sia competente per le varie misure volte a trattare i rischi e a proteggere i diritti e le libertà degli interessati. Ciascun titolare del trattamento deve esprimere le proprie esigenze e condividere informazioni utili senza compromettere eventuali segreti (ad esempio protezione di segreti aziendali, proprietà intellettuale, informazioni aziendali riservate) o divulgare vulnerabilità.

Una valutazione d'impatto sulla protezione dei dati può essere altresì utile per valutare l'impatto sulla protezione dei dati di un prodotto tecnologico, ad esem-

pio un dispositivo hardware o un software, qualora sia probabile che lo stesso venga utilizzato da titolari del trattamento distinti per svolgere tipologie diverse di trattamento. Ovviamente, il titolare del trattamento che utilizza detto prodotto resta soggetto all'obbligo di svolgere la propria valutazione d'impatto sulla protezione dei dati in relazione all'attuazione specifica, tuttavia tale valutazione del titolare del trattamento può utilizzare le informazioni fornite da una valutazione analoga preparata dal fornitore del prodotto, se opportuno. Un esempio potrebbe essere rappresentato dalla relazione tra produttori di contatori intelligenti e società fornitrici di servizi pubblici. Ogni fornitore di prodotti o responsabile del trattamento dovrebbe condividere informazioni utili senza compromettere i segreti né generare rischi per la sicurezza, divulgando vulnerabilità.

B. QUALI TRATTAMENTI SONO SOGGETTI A UNA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI? ESCLUDENDO LE ECCEZIONI, IN TUTTI I CASI IN CUI TALI TRATTAMENTI *"POSSONO PRESENTARE UN RISCHIO ELEVATO"*.

Questa sezione descrive i casi nei quali è richiesta una valutazione d'impatto sulla protezione dei dati e quelli che invece non la richiedono.

Fatti salvi i casi in cui un trattamento rientra nel campo di applicazione di un'eccezione (III.B.a), è necessario realizzare una valutazione d'impatto sulla protezione dei dati qualora un trattamento *"possa presentare un rischio elevato"* **(III.B.b).**

a) Quando è obbligatoria una valutazione d'impatto sulla protezione dei dati? Quando il trattamento *"può presentare un rischio elevato"*.

Il regolamento generale sulla protezione dei dati non richiede la realizzazione di una valutazione d'impatto sulla protezione dei dati per ciascun trattamento che può presentare rischi per i diritti e le libertà delle persone fisiche. La realizzazione di una valutazione d'impatto sulla protezione dei dati è obbligatoria soltanto qualora il trattamento *"possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche"* (articolo 35, paragrafo 1, illustrato dall'articolo 35, paragrafo 3, e integrato dall'articolo 35, paragrafo 4). Essa è particolarmente importante quando viene introdotta una nuova tecnologia di trattamento dei dati[11].

Nei casi in cui non è chiaro se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno, il WP29 raccomanda di effettuarla comunque, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati.

Sebbene una valutazione d'impatto sulla protezione dei dati possa essere richiesta anche in altre circostanze, l'articolo 35, paragrafo 3, fornisce alcuni esempi di casi nei quali un trattamento "possa presentare rischi elevati":

- *"a) una valutazione sistematica e globale di aspetti personali relativi a persone*

fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche[12]*;*

- *b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10*[13]*; o*
- *c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".*

Come indicato dalle parole "in particolare" nella frase introduttiva dell'articolo 35, paragrafo 3, del regolamento generale sulla protezione dei dati, questo va inteso come un elenco non esaustivo. Vi possono essere operazioni di trattamento a "rischio elevato" che non trovano collocazione in tale elenco ma che presentano tuttavia rischi altrettanto elevati. Anche tali trattamenti devono essere soggetti alla realizzazione di valutazioni d'impatto sulla protezione dei dati. Per questo motivo, i criteri sviluppati qui di seguito vanno, talvolta, al di là di una semplice spiegazione dell'interpretazione dei tre esempi di cui all'articolo 35, paragrafo 3, del regolamento generale sulla protezione dei dati.

Al fine di fornire un insieme più concreto di trattamenti che richiedono una valutazione d'impatto sulla protezione dei dati in virtù del loro rischio elevato intrinseco, tenendo conto degli elementi particolari di cui all'articolo 35, paragrafo 1 e all'articolo 35, paragrafo 3, lettere da a) a c), l'elenco da adottare a livello nazionale ai sensi dell'articolo 35, paragrafo 4, e dei considerando 71, 75 e 91, e di altri riferimenti del regolamento generale sulla protezione dei dati a trattamenti che *"possono presentare un rischio elevato"*[14], si devono considerare i seguenti nove criteri.

1. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di *"aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"* (considerando 71 e 91). Esempi di ciò potrebbero includere: un ente finanziario che esamina i suoi clienti rispetto a una banca dati di riferimento in materia di crediti oppure rispetto a una banca dati in materia di lotta contro il riciclaggio e il finanziamento del terrorismo (AML/CTF) oppure contenente informazioni sulle frodi; oppure un'impresa di biotecnologie che offre test genetici direttamente ai consumatori per valutare e prevedere i rischi di malattia o per la salute; oppure un'impresa che crea profili comportamentali o per la commercializzazione basati sull'utilizzo del proprio sito web o sulla navigazione sullo stesso;

2. processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che *"hanno effetti giuridici"* o che *"incidono in modo analogo significativamente su dette persone fisiche"* (articolo 35, paragrafo 3, lettera a)). Ad esempio, il trattamento può portare all'esclu-

sione o alla discriminazione nei confronti delle persone. Il trattamento che non ha effetto o ha soltanto un effetto limitato sulle persone non risponde a questo criterio specifico. Ulteriori spiegazioni in merito a queste nozioni saranno fornite nelle linee guida sulla profilazione che saranno pubblicate prossimamente dal WP29;

3. monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o *"la sorveglianza sistematica su larga scala di una zona accessibile al pubblico"* (articolo 35, paragrafo 3, lettera c))[15]. Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);

4. dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10. Un esempio potrebbe essere quello di un ospedale generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone;

5. trattamento di dati su larga scala: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccoman-

da di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala[16]:

a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
c. la durata, ovvero la persistenza, dell'attività di trattamento;
d. la portata geografica dell'attività di trattamento;

6. creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato[17];

7. dati relativi a interessati vulnerabili (considerando 75): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;

8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc. Il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita *"in conformità con il grado di conoscenze tecnologiche raggiunto"* (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi. Ad esempio, alcune applicazioni di "Internet delle cose" potrebbero avere un impatto significativo sulla vita quotidiana e sulla vita privata delle persone e, di conseguenza, richiedono la realizzazione di una valutazione d'impatto sulla protezione dei dati;

9. quando il trattamento in sé *"impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto"* (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto.

Un esempio di ciò è rappresentato dal caso in cui una banca esamina i suoi clienti rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno.

Nella maggior parte dei casi, un titolare del trattamento può considerare che un trattamento che soddisfi due criteri debba formare oggetto di una valutazione d'impatto sulla protezione dei dati. In generale, il WP29 ritiene che maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati, indipendentemente dalle misure che il titolare del trattamento ha previsto di adottare.

Tuttavia, in alcuni casi, **un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno di questi criteri richieda una valutazione d'impatto sulla protezione dei dati.**

Gli esempi riportati di seguito illustrano come utilizzare i criteri per valutare se una particolare tipologia di trattamento richieda una valutazione d'impatto sulla protezione dei dati o meno.

Esempi di trattamento	Possibili criteri pertinenti	È probabile che sia richiesta una valutazione d'impatto sulla protezione dati?
Un ospedale che tratta i dati genetici e sanitari dei propri pazienti (sistema informativo ospedaliero).	• Dati sensibili o dati aventi carattere estremamente personale. • Dati riguardanti soggetti interessati vulnerabili. • Trattamento di dati su larga scala.	Si
L'uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade. Il titolare del trattamento prevede di utilizzare un sistema intelligente di analisi video per individuare le auto e riconoscere automaticamente le targhe.	• Monitoraggio sistematico. • Uso innovativo o applicazione di soluzioni tecnologiche od organizzative.	

Un'azienda che monitora sistematicamente le attività dei suoi dipendenti, controllando anche la postazione di lavoro dei dipendenti, le loro attività in Internet, ecc.	• Monitoraggio sistematico. • Dati riguardanti soggetti interessati vulnerabili.	Si
La raccolta di dati pubblici dei media sociali per la generazione di profili.	• Valutazione o assegnazione di un punteggio. • Trattamento di dati su larga scala. • Creazione di corrispondenze o combinazione di insiemi di dati. • Dati sensibili o dati aventi carattere estremamente personale.	
Un'istituzione che crea una banca dati antifrode e di gestione del rating del credito a livello nazionale.	• Valutazione o assegnazione di un punteggio. • Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente. • Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto. • Dati sensibili o dati aventi carattere estremamente personale.	
Conservazione per finalità di archiviazione di dati sensibili personali pseudonimizzati relativi a interessati vulnerabili coinvolti in progetti di ricerca o sperimentazioni cliniche.	• Dati sensibili. • Dati riguardanti soggetti interessati vulnerabili. • Impedisce agli interessati di esercitare un diritto utilizzare un servizio o un contratto.	

Un trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato" (considerando 91).	• Dati sensibili o dati aventi carattere estremamente personale. • Dati riguardanti soggetti interessati vulnerabili.	No
Una rivista online che utilizza una lista di distribuzione per inviare una selezione quotidiana generica ai suoi abbonati.	• Trattamento di dati su larga scala.	
Un sito web di commercio elettronico che visualizza annunci pubblicitari per parti di auto d'epoca che comporta una limitata profilazione basata sugli articoli visualizzati o acquistati sul proprio sito web.	• Valutazione o assegnazione di un punteggio.	

Per contro, un trattamento può corrispondere ai casi di cui sopra ed essere comunque considerato dal titolare del trattamento un trattamento tale da non "presentare un rischio elevato". In tali casi il titolare del trattamento deve giustificare e documentare i motivi che lo hanno spinto a non effettuare una valutazione d'impatto sulla protezione dei dati, nonché includere/registrare i punti di vista del responsabile della protezione dei dati.

Inoltre, nel contesto del principio di responsabilizzazione, ogni titolare del trattamento deve tenere *"un registro delle attività di trattamento svolte sotto la propria responsabilità"* che includa, tra l'altro, le finalità del trattamento, una descrizione delle categorie di dati e di destinatari dei dati e *"ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1"* (articolo 30, paragrafo 1); inoltre, deve valutare la probabilità di un rischio elevato, anche qualora decida in ultima analisi di non realizzare una valutazione d'impatto sulla protezione dei dati.

Nota: le autorità di controllo sono tenute a stabilire, rendere pubblico e comunicare al comitato europeo per la protezione dei dati un elenco delle tipologie di trattamento che richiedono una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 4)[18]. I criteri di cui sopra possono aiutare le autorità di controllo a redigere un tale elenco, aggiungendo contenuti specifici nel corso del tempo, se applicabile. Ad esempio, anche il trattamento di qualsiasi tipo di dati biometrici o di dati di minori potrebbe essere considerato pertinente per lo sviluppo di un elenco ai sensi dell'articolo 35, paragrafo 4.

b) Quando non è richiesta una valutazione d'impatto sulla protezione dei dati? Quando il trattamento non è tale da "presentare un rischio elevato" oppure qualora esista una valutazione d'impatto sulla protezione dei dati analoga, o qualora il trattamento sia stato autorizzato prima del maggio 2018 oppure abbia una base giuridica o sia incluso nell'elenco delle tipologie di trattamento per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati.

Il WP29 ritiene che una valutazione d'impatto sulla protezione dei dati non sia richiesta nei seguenti casi:

- **quando il trattamento non è tale da *"presentare un rischio elevato per i diritti e le libertà delle persone fisiche"*** (articolo 35, paragrafo 1);
- **quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati.** In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo (articolo 35, paragrafo 1[19]);
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate[20] (cfr. III.C);
- **qualora un trattamento**, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e), trovi **una base giuridica** nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o **sia già stata effettuata una valutazione d'impatto sulla protezione dei dati** nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10)[21], a meno che uno Stato membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento;
- **qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento** per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5). Tale elenco può contenere attività di trattamento conformi alle condizioni specificate da detta autorità, in particolare attraverso linee guida, decisioni o autorizzazioni specifiche, norme di conformità, ecc. (ad esempio in Francia, autorizzazioni, esenzioni, norme semplificate, pacchetti di conformità, ecc.). In tali casi e a condizione che venga eseguita una nuova valutazione da parte dell'autorità di controllo competente, non è richiesta una valutazione d'impatto sulla protezione dei dati, ma soltanto se il trattamento rientra a tutti gli effetti nel campo di applicazione della procedura pertinente menzionata nell'elenco e continua a rispettare pienamente tutti i requisiti pertinenti del regolamento generale sulla protezione dei dati.

C. QUALE REGOLA SI APPLICA AI TRATTAMENTI GIÀ ESISTENTI? IN TALUNE CIRCOSTANZE SONO RICHIESTE VALUTAZIONI D'IMPATTO SULLA PROTEZIONE DEI DATI.

L'obbligo di svolgere una valutazione d'impatto sulla protezione dei dati si applica alle operazioni di trattamento esistenti che possono presentare un

rischio elevato per i diritti e le libertà delle persone fisiche e per le quali vi è stata una variazione dei rischi, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.

Non è necessaria una valutazione d'impatto sulla protezione dei dati per i trattamenti che sono stati verificati da un'autorità di controllo o dal responsabile della protezione dei dati, a norma dell'articolo 20 della direttiva 95/46/CE e che vengono eseguiti in maniera tale da fare sì che non si sia registrata alcuna variazione rispetto alla verifica precedente. In effetti, *"[l]e decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate"* (considerando 171).

Al contrario, ciò significa che qualsiasi trattamento di dati le cui condizioni di attuazione (ambito di applicazione, finalità, dati personali raccolti, identità dei titolari del trattamento o dei destinatari, periodo di conservazione dei dati, misure tecniche e organizzative, ecc.) sono mutate rispetto alla prima verifica effettuata dall'autorità di controllo o dal responsabile della protezione dei dati e che possono presentare un rischio elevato devono essere soggette a una valutazione d'impatto sulla protezione dei dati.

Inoltre, potrebbe essere richiesta una valutazione d'impatto sulla protezione dei dati in seguito a una variazione dei rischi derivante dalle operazioni di trattamento[22], ad esempio perché è entrata in uso una nuova tecnologia o perché i dati personali vengono utilizzati per una finalità diversa. Le operazioni di trattamento dei dati possono evolversi rapidamente e potrebbero emergere nuove vulnerabilità. Di conseguenza, va osservato che la revisione di una valutazione d'impatto sulla protezione dei dati non è utile soltanto ai fini di un miglioramento continuo, bensì anche fondamentale per mantenere il livello di protezione dei dati in un ambiente che muta nel corso del tempo. Una valutazione d'impatto sulla protezione dei dati potrebbe rendersi necessaria anche perché il contesto organizzativo o sociale per l'attività di trattamento è mutato, ad esempio perché gli effetti di determinate decisioni automatizzate sono diventati più significativi oppure perché nuove categorie di interessati sono diventati vulnerabili alla discriminazione. Ciascuno di questi esempi potrebbe costituire un aspetto che porta a una variazione del rischio derivante dall'attività di trattamento interessata.

Al contrario, talune modifiche potrebbero anche ridurre il rischio. Ad esempio, un trattamento potrebbe evolvere in modo tale da fare sì che le decisioni non siano più automatizzate oppure si pensi al caso in cui un'attività di monitoraggio non viene più eseguita in maniera sistematica. In questo caso, il riesame dell'analisi dei rischi può mostrare che non è più necessario eseguire una valutazione d'impatto sulla protezione dei dati.

Secondo le buone prassi, **una valutazione d'impatto sulla protezione dei dati va riesaminata continuamente e rivalutata con regolarità.** Di conseguenza, anche se una valutazione d'impatto sulla protezione dei dati non è richiesta il

25 maggio 2018, al momento opportuno, il titolare del trattamento sarà tenuto a svolgere tale valutazione nel contesto dei suoi obblighi generali di responsabilizzazione.

D. COME VA SVOLTA UNA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI?

a) In quale momento va effettuata una valutazione d'impatto sulla protezione dei dati? Prima del trattamento.

La valutazione d'impatto sulla protezione dei dati va effettuata "prima del trattamento" (articolo 35, paragrafi 1 e 10, considerando 90 e 93)[23]. Ciò è coerente con i principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita (articolo 25 e considerando 78). La valutazione d'impatto sulla protezione dei dati va considerata come uno strumento atto a contribuire al processo decisionale in materia di trattamento.

La valutazione d'impatto sulla protezione dei dati va avviata il prima possibile nella fase di progettazione del trattamento anche se alcune delle operazioni di trattamento non sono ancora note. L'aggiornamento della valutazione d'impatto sulla protezione dei dati nel corso dell'intero ciclo di vita del progetto garantirà che la protezione dei dati e della vita privata sia presa in considerazione e favorisca la creazione di soluzioni che promuovono la conformità. Può essere altresì necessario ripetere singole fasi della valutazione man mano che il processo di sviluppo evolve, dato che la selezione di determinate misure tecniche od organizzative può influenzare la gravità o la probabilità dei rischi posti dal trattamento.
Il fatto che possa rendersi necessario aggiornare la valutazione d'impatto sulla protezione dei dati dopo l'effettivo avvio del trattamento non costituisce un motivo valido per rinviare o non svolgere una valutazione d'impatto sulla protezione dei dati. La valutazione d'impatto sulla protezione dei dati è un processo continuo, soprattutto quando un trattamento è dinamico ed è soggetto a variazioni continue.

Realizzare una valutazione d'impatto sulla protezione dei dati è un processo continuo, non un esercizio *una tantum*.

b) Chi è obbligato a effettuare la valutazione d'impatto sulla protezione dei dati? Il titolare del trattamento, con il responsabile della protezione dei dati e i responsabili del trattamento.

Al titolare del trattamento spetta assicurare che la valutazione d'impatto sulla protezione dei dati sia eseguita (articolo 35, paragrafo 2). La valutazione d'impatto sulla protezione dei dati può essere effettuata da qualcun altro, all'interno o all'esterno dell'organizzazione, tuttavia al titolare del trattamento spetta la responsabilità ultima per tale compito.

Inoltre il titolare del trattamento deve consultarsi con il responsabile della protezione dei dati (RPD), qualora ne sia designato uno (articolo 35, paragrafo 2) e il parere ricevuto, così come le decisioni prese dal titolare del trattamento, debbano essere documentate all'interno della valutazione d'impatto sulla protezione dei dati. Il responsabile della protezione dei dati deve altresì sorvegliare lo svolgimento della valutazione d'impatto sulla protezione dei dati (articolo 39, paragrafo 1, lettera c)). Ulteriori orientamenti in merito sono forniti nelle "Linee guida sui responsabili della protezione dei dati (RPD)" del WP29 - 16/EN WP 243.

Qualora il trattamento venga eseguito in toto o in parte da un responsabile del trattamento dei dati, **quest'ultimo deve assistere il titolare del trattamento nell'esecuzione della valutazione d'impatto sulla protezione dei dati** e fornire tutte le informazioni necessarie (conformemente all'articolo 28, paragrafo 3, lettera f)).

Il titolare del trattamento deve *"raccoglie[re] le opinioni degli interessati o dei loro rappresentanti"* (articolo 35, paragrafo 9), *"se del caso"*. Il WP29 ritiene che:

- tali opinioni possono essere raccolte attraverso una varietà di mezzi, a seconda del contesto (ad esempio uno studio generico relativo alla finalità e ai mezzi del trattamento, una domanda posta ai rappresentanti del personale oppure indagini abituali inviate ai futuri clienti del titolare del trattamento), assicurando che il titolare del trattamento disponga di una base giuridica valida per il trattamento di qualsiasi dato personale interessato nel raccogliere dette opinioni; sebbene sia opportuno osservare che il consenso al trattamento non è ovviamente un modo per raccogliere le opinioni degli interessati;
- qualora la decisione finale del titolare del trattamento si discosti dalle opinioni degli interessati, le sue motivazioni a sostegno del procedere o meno vanno documentate;
- il titolare del trattamento deve altresì documentare la sua giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che ciò non sia appropriato, ad esempio qualora ciò comporterebbe la riservatezza dei piani economici dell'impresa o sarebbe sproporzionato o impraticabile.

Infine, è buona prassi definire e documentare altri ruoli e responsabilità specifici, a seconda delle politiche, dei processi e delle norme interni, ad esempio:

- qualora specifiche unità aziendali propongano di svolgere una valutazione d'impatto sulla protezione dei dati, tali unità dovrebbero poi fornire contributi alla valutazione d'impatto sulla protezione dei dati ed essere coinvolte nel processo di convalida di detta valutazione;
- se del caso, si raccomanda di consultare esperti indipendenti che esercitano professioni diverse[24] (avvocati, esperti informatici, esperti di sicurezza, sociologi, esperti di etica, ecc.);
- i ruoli e le responsabilità dei responsabili del trattamento devono essere definiti contrattualmente; e la valutazione d'impatto sulla protezione dei dati deve essere svolta con l'assistenza di un responsabile del trattamento, te-

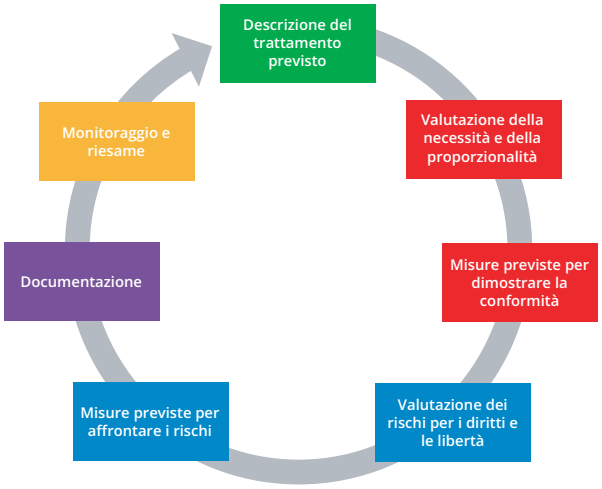
nendo conto della natura del trattamento e delle informazioni a disposizione di detto responsabile del trattamento (articolo 28, paragrafo 3, lettera f));
- il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, così come il responsabile della protezione dei dati, potrebbero suggerire al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento e dovrebbero assistere le parti interessate in relazione alla metodologia, contribuire alla valutazione della qualità della valutazione dei rischi e del grado di accettabilità del rischio residuo, nonché allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
- il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione, dovrebbero fornire assistenza al titolare del trattamento, nonché potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza.

c) Qual è la metodologia da seguire per svolgere una valutazione d'impatto sulla protezione dei dati? Vi sono metodologie diverse, ma criteri comuni.

Il regolamento generale sulla protezione dei dati definisce le caratteristiche minime di una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 7, e considerando 84 e 90):

- *"una descrizione dei trattamenti previsti e delle finalità del trattamento"*;
- *"una valutazione della necessità e proporzionalità dei trattamenti"*;
- *"una valutazione dei rischi per i diritti e le libertà degli interessati"*;
- *"le misure previste per"*:
  - *"affrontare i rischi"*;
  - *"dimostrare la conformità al presente regolamento"*.

La figura che segue illustra il processo iterativo generico per lo svolgimento di una valutazione d'impatto sulla protezione dei dati[25]:



Nel valutare l'impatto di un trattamento va tenuto conto (articolo 35, paragrafo 8) del rispetto di un codice di condotta (articolo 40). Ciò può essere utile per dimostrare che sono state scelte o messe in atto misure adeguate, a condizione che il codice di condotta sia adeguato all'operazione di trattamento interessata. Devono essere presi in considerazione anche certificazioni, sigilli e marchi al fine di dimostrare la conformità rispetto al regolamento generale sulla protezione dei dati dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento (articolo 42), nonché rispetto alle norme vincolanti d'impresa.

Tutti i requisiti pertinenti stabiliti nel regolamento generale sulla protezione dei dati offrono un quadro ampio e generico per la progettazione e lo svolgimento di una valutazione d'impatto sulla protezione dei dati. L'attuazione pratica di una valutazione d'impatto sulla protezione dei dati dipenderà dai requisiti stabiliti nel regolamento generale sulla protezione dei dati che possono essere integrati da orientamenti pratici più dettagliati. L'attuazione della valutazione d'impatto sulla protezione dei dati è quindi modulabile. Ciò significa che anche un titolare del trattamento di piccole dimensioni può progettare e attuare una valutazione d'impatto sulla protezione dei dati adatta ai propri trattamenti.

Il considerando 90 del regolamento generale sulla protezione dei dati delinea una serie di elementi costituivi della valutazione d'impatto sulla protezione dei dati che si sovrappone a elementi ben definiti della gestione del rischio (ad esempio norma ISO 31000[26]). In termini di gestione dei rischi, una valutazione d'impatto sulla protezione dei dati mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche, utilizzando i seguenti processi:

- stabilendo il contesto: *"tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio"*;
- valutando i rischi: *"valutare la particolare probabilità e gravità del rischio"*;
- trattando i rischi: *"atten[uando] tale rischio"* e *"assicurando la protezione dei dati personali"*, e *"dimostrando la conformità al presente regolamento"*.

Nota: la valutazione d'impatto sulla protezione dei dati svolta ai sensi del regolamento generale sulla protezione dei dati è uno strumento per gestire i rischi per i diritti degli interessati, di conseguenza, adotta la loro prospettiva, come avviene in taluni settori (ad esempio, la sicurezza sociale). Al contrario, la gestione del rischio in altri settori (ad esempio in quello della sicurezza delle informazioni) è incentrata sull'organizzazione.

Il regolamento generale sulla protezione dei dati offre ai titolari del trattamento la flessibilità di stabilire la struttura e la forma precise della valutazione d'impatto sulla protezione dei dati in maniera da consentire che la stessa si adatti alle pratiche di lavoro esistenti. Esistono diversi processi stabiliti all'interno dell'UE e nel mondo che tengono conto degli elementi costitutivi descritti nel considerando 90. Tuttavia, indipendentemente dalla sua forma, una valutazione d'impatto sulla protezione dei dati deve essere una vera e propria va-

lutazione dei rischi che consenta ai titolari del trattamento di adottare misure per affrontarli.

Si potrebbe ricorrere a metodologie diverse (cfr. allegato 1 per esempi di metodologie di valutazione dell'impatto sulla vita privata e sulla protezione dei dati) per contribuire all'attuazione dei requisiti essenziali stabiliti nel regolamento generale sulla protezione dei dati. Al fine di consentire l'esistenza di tali approcci distinti, permettendo comunque ai titolari del trattamento di rispettare il regolamento generale sulla protezione dei dati, sono stati individuati dei criteri comuni (cfr. allegato 2). Tali criteri chiariscono i requisiti essenziali del regolamento, ma offrono un campo di applicazione sufficiente da consentire la coesistenza di forme diverse di attuazione. Detti criteri possono essere utilizzati per dimostrare che una particolare metodologia di valutazione d'impatto sulla protezione dei dati soddisfa i parametri imposti dal regolamento generale sulla protezione dei dati. **Spetta al titolare del trattamento scegliere una metodologia che, comunque, deve essere conforme ai criteri di cui all'allegato 2.**

Il WP29 incoraggia lo sviluppo di quadri di valutazione d'impatto sulla protezione dei dati specifici dei vari settori. Ciò è dovuto al fatto che essi possono attingere a conoscenze specifiche settoriali, aspetto questo che fa sì che la valutazione d'impatto sulla protezione dei dati possa affrontare le specificità di un particolare tipo di trattamento (ad esempio tipi particolari di dati, risorse aziendali, impatti potenziali, minacce, misure). Ciò significa che la valutazione d'impatto sulla protezione dei dati può affrontare le problematiche che sorgono in un settore economico specifico oppure quando si utilizzano tecnologie particolari o si eseguono tipologie particolari di trattamento.

Infine, se necessario, "il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento" (articolo 35, paragrafo 11[27]).

d) Esiste l'obbligo di pubblicare la valutazione d'impatto sulla protezione dei dati? No, tuttavia pubblicarne una sintesi potrebbe favorire la fiducia e la valutazione d'impatto sulla protezione dei dati completa deve essere comunicata all'autorità di controllo in caso di consultazione preventiva o su richiesta da parte delle autorità competenti per la protezione dei dati personali.

La pubblicazione di una valutazione d'impatto sulla protezione dei dati non è un requisito giuridico sancito dal regolamento generale sulla protezione dei dati, è una decisione del titolari del trattamento procedere in tal senso. Tuttavia, i titolari del trattamento dovrebbero prendere in considerazione la pubblicazione di almeno alcune parti, ad esempio di una sintesi o della conclusione della loro valutazione d'impatto sulla protezione dei dati.

Lo scopo di un tale processo sarebbe quello di contribuire a stimolare la fiducia nei confronti dei trattamenti effettuati dal titolare del trattamento, nonché di dimostrare la responsabilizzazione e la trasparenza. Costituisce una prassi particolarmente buona pubblicare una valutazione d'impatto sulla protezione dei dati nel caso in cui individui della popolazione siano influenzati dal trattamento interessato. Nello specifico, ciò potrebbe essere il caso in cui un'autorità pubblica realizza una valutazione d'impatto sulla protezione dei dati.

La valutazione d'impatto sulla protezione dei dati pubblicata non deve necessariamente contenere l'intera valutazione, soprattutto qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza per il titolare del trattamento o divulgare segreti commerciali o informazioni commerciali sensibili. In queste circostanze, la versione pubblicata potrebbe consistere soltanto in una sintesi delle principali risultanze della valutazione d'impatto sulla protezione dei dati o addirittura soltanto in una dichiarazione nella quale si afferma che la valutazione d'impatto sulla protezione dei dati è stata condotta.

Inoltre, laddove una valutazione d'impatto sulla protezione dei dati riveli la presenza di rischi residui elevati, il titolare del trattamento sarà tenuto a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento (articolo 36, paragrafo 1). In tale contesto, la valutazione d'impatto sulla protezione dei dati deve essere fornita completa (articolo 36, paragrafo 3, lettera e)).

L'autorità di controllo può fornire il proprio parere[28] e procurerà di non compromettere segreti commerciali né divulgare vulnerabilità di sicurezza, in conformità con i principi applicabili in ciascuno Stato membro in materia di accesso del pubblico a documenti ufficiali.

E. QUANDO È NECESSARIO CONSULTARE L'AUTORITÀ DI CONTROLLO? QUANDO I RISCHI RESIDUI SONO ELEVATI

Come spiegato in precedenza:

- è necessario realizzare una valutazione d'impatto sulla protezione dei dati quando il trattamento *"può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"* (articolo 35, paragrafo 1; cfr. III.B.a). A titolo di esempio, il trattamento di dati sanitari su larga scala è considerato un trattamento tale da presentare un rischio elevato e richiede la realizzazione di una valutazione d'impatto sulla protezione dei dati;
- di conseguenza, spetta al titolare del trattamento valutare i rischi per i diritti e le libertà degli interessati e individuale le misure[29] previste per attenuare tali rischi a un livello accettabile e per dimostrare la conformità rispetto al regolamento generale sulla protezione dei dati (articolo 35, paragrafo 7; cfr. III.C.c). un esempio, in caso di conservazione di dati personali su computer portatili, potrebbe essere l'utilizzo di adeguate misure di sicurezza tecniche e organizzative (crittografia efficace completa del di-

sco, gestione di chiavi robuste, opportuno controllo degli accessi, backup protetti, ecc.) oltre al ricorso a politiche esistenti (avviso, consenso, diritto di accesso, diritto di opposizione, ecc.).

Nell'esempio sopra riportato relativo ai computer portatili, qualora i rischi siano stati considerati sufficientemente attenuati dal titolare del trattamento e in seguito alla lettura dell'articolo 36, paragrafo 1 e dei considerando 84 e 94, il trattamento può procedere senza la consultazione dell'autorità di controllo. È nei casi in cui il titolare del trattamento non riesca a trattare in maniera sufficiente i rischi individuati (ossia i rischi residui rimangono elevati) che questi deve consultare l'autorità di controllo.

Un esempio di un rischio residuo elevato inaccettabile include casi in cui gli interessati possano subire conseguenze significative, o addirittura irreversibili, che non possono superare (ad esempio: accesso illegittimo a dati che comportano una minaccia per la vita degli interessati, un loro licenziamento, un rischio finanziario) e/o quando appare evidente che il rischio si verificherà (ad esempio: poiché non si è in grado di ridurre il numero di persone che accedono ai dati a causa delle loro modalità di condivisione, utilizzo o distribuzione o quando non si può porre rimedio a una vulnerabilità ben nota).

Ogniqualvolta il titolare del trattamento non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati) è necessario consultare l'autorità di controllo[30].

Inoltre, il titolare del trattamento dovrà consultare l'autorità di vigilanza qualora il diritto dello Stato membro in questione prescriva che i titolari del trattamento consultino l'autorità di controllo e/o ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica (articolo 36, paragrafo 5).

Occorre tuttavia sottolineare che, indipendentemente dal fatto che la consultazione dell'autorità di controllo sia richiesta o meno in base al livello di rischio residuo, sussistono comunque gli obblighi di conservare una registrazione della valutazione d'impatto sulla protezione dei dati e di aggiornamento di detta valutazione al momento opportuno.

IV. CONCLUSIONI E RACCOMANDAZIONI

Le valutazioni d'impatto sulla protezione dei dati sono uno strumento utile di cui dispongono i titolari del trattamento per attuare sistemi di trattamento dei dati conformi al regolamento generale sulla protezione dei dati e possono essere obbligatorie per talune tipologie di trattamenti. Hanno natura modulabile e possono assumere forme diverse, tuttavia il regolamento generale sulla protezione dei dati stabilisce i requisiti essenziali di una valutazione d'impatto sulla

protezione dei dati efficace. I titolari del trattamento dovrebbero considerare la realizzazione di una valutazione d'impatto sulla protezione dei dati come un'attività utile e positiva che contribuisce alla conformità giuridica.

L'articolo 24, paragrafo 1, definisce la responsabilità fondamentale del titolare del trattamento in termini di rispetto del regolamento generale sulla protezione dei dati: *"Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario"*.

La valutazione d'impatto sulla protezione dei dati è un aspetto fondamentale del rispetto del regolamento laddove si preveda di svolgere o si stia svolgendo un trattamento di dati soggetto a rischio elevato. Ciò significa che i titolari del trattamento dovrebbero utilizzare i criteri stabiliti nel presente documento per stabilire se devono realizzare una valutazione d'impatto sulla protezione dei dati o meno. La politica interna dei titolari del trattamento potrebbe estendere questo elenco andando oltre i requisiti giuridici sanciti dal regolamento generale sulla protezione dei dati. Ciò dovrebbe suscitare un maggior senso di fiducia e riservatezza negli interessati e in altri titolari del trattamento.

Qualora si preveda di effettuare un trattamento che possa presentare un rischio elevato, il titolare del trattamento deve:

- scegliere una metodologia per la valutazione d'impatto sulla protezione dei dati (esempi riportati nell'allegato 1) che soddisfi i criteri di cui all'allegato 2, oppure specificare ed attuare un processo sistematico di valutazione d'impatto sulla protezione dei dati che:
  - sia conforme ai criteri di cui all'allegato 2;
  - sia integrata nei processi in materia di progettazione, sviluppo, cambiamento, rischio e riesame operativo in conformità con i processi, il contesto e la cultura interni;
  - coinvolga le parti interessate appropriate e definisca chiaramente le loro responsabilità (titolare del trattamento, responsabile della protezione dei dati, interessati o loro rappresentanti, imprese, servizi tecnici, responsabili del trattamento, responsabile della sicurezza dei sistemi d'informazione, ecc.);
- fornire la relazione relativa alla valutazione d'impatto sulla protezione dei dati all'autorità di controllo, laddove gli venga richiesto di procedere in tal senso;
- consultare l'autorità di controllo, qualora il titolare del trattamento non sia riuscito a determinare misure sufficienti per attenuare i rischi elevati;
- riesaminare periodicamente la valutazione d'impatto sulla protezione dei dati e il trattamento che essa valuta, almeno quando si registra una variazione del rischio posto dal trattamento;
- documentare le decisioni prese.

ALLEGATO 1
ESEMPI DI QUADRI UE ESISTENTI DI VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Il regolamento generale sulla protezione dei dati non specifica quale processo di valutazione d'impatto sulla protezione dei dati debba essere seguito, ma consente piuttosto ai titolari del trattamento di introdurre un quadro che integri le loro pratiche di lavoro esistenti, purché tenga conto degli elementi costitutivi di cui all'articolo 35, paragrafo 7. Tale quadro può essere personalizzato per lo specifico titolare del trattamento oppure essere comune a un determinato settore. I quadri precedentemente pubblicati sviluppati dalle autorità di protezione dei dati dell'UE e i quadri specifici di settore dell'UE includono (elenco non esaustivo):

esempi di quadri generici dell'UE:

- DE: modello per la protezione dei dati standard, V.1.0 - versione di prova, 2016[31].
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf;
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Gui a_EIPD.pdf;
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/node/15798;
- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf;

esempi di quadri UE specifici di settore:

- *Privacy and Data Protection Impact Assessment Framework for RFID Applications*
  [Quadro per la realizzazione di valutazioni di impatto sulla protezione della vita privata e dei dati per le applicazioni RFID][32].
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf;
- *Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems*
  [Modello per la valutazione d'impatto sulla protezione dei dati per la rete intelligente e i sistemi di misurazione intelligenti][33]
  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf.

Anche una norma internazionale fornirà orientamenti in merito alle metodologie utilizzate per la realizzazione di una valutazione d'impatto sulla protezione dei dati (ISO/IEC 29134[34]).

ALLEGATO 2

CRITERI PER UNA VALUTAZIONE D'IMPATTO

SULLA PROTEZIONE DEI DATI ACCETTABILE

Il WP29 propone i seguenti criteri che i titolari del trattamento possono utilizzare per stabilire se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno oppure se una metodologia per lo svolgimento di una tale valutazione sia sufficientemente completa per garantire il rispetto del regolamento generale sulla protezione dei dati:

- ❏ una descrizione sistematica del trattamento è fornita (articolo 35, paragrafo 7, lettera a)):
  - ❏ la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);
  - ❏ vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
  - ❏ viene fornita una descrizione funzionale del trattamento;
  - ❏ sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);
  - ❏ si tiene conto del rispetto dei codici di condotta approvati (articolo 35, paragrafo 8);
- ❏ la necessità e la proporzionalità sono valutate (articolo 35, paragrafo 7, lettera b)):
  - ❏ sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):
    - ❏ misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
      - ❏ finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));
      - ❏ liceità del trattamento (articolo 6);
      - ❏ dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));
      - ❏ limitazione della conservazione (articolo 5, paragrafo 1, lettera e));
    - ❏ misure che contribuiscono ai diritti degli interessati:
      - ❏ informazioni fornite all'interessato (articoli 12, 13 e 14);
      - ❏ diritto di accesso e portabilità dei dati (articoli 15 e 20);
      - ❏ diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);
      - ❏ diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);
      - ❏ rapporti con i responsabili del trattamento (articolo 28);
      - ❏ garanzie riguardanti trattamenti internazionali (capo V);
      - ❏ consultazione preventiva (articolo 36).
- ❏ i rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c)):

- ❏ l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:
  - ❏ si considerano le fonti di rischio (considerando 90);
  - ❏ sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
  - ❏ sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;
  - ❏ sono stimate la probabilità e la gravità (considerando 90);
- ❏ sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90);

- ❏ le parti interessate sono coinvolte:
  - ❏ si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2);
  - ❏ si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo 9).

NOTE

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[2] In altri contesti il termine "valutazione dell'impatto sulla vita privata" è spesso utilizzato per fare riferimento allo stesso concetto.

[3] L'articolo 27 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, prevede altresì che sia necessaria una valutazione dell'impatto sulla vita privata *"quando il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"*.

[4] Il regolamento generale sulla protezione dei dati non definisce formalmente il concetto di valutazione d'impatto sulla protezione dei dati come tale, tuttavia

- il suo contenuto minimo è specificato dall'articolo 35, paragrafo 7, come segue:
  "a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
  b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
  c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
  d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione";
- il suo significato e il suo ruolo sono chiariti dal considerando 84 come segue: *"[p]er potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio"*.

[5] Cfr. anche il considerando 84: *"[l]'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento"*.

[6] *"WP29 Statement 14/EN WP 218 on the role of a risk-based approach to data protection legal frameworks"* [Dichiarazione del WP29 14/EN WP 218 sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati], adottata il 30 maggio 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/ wp218_en.pdf?wb48617274=72C54532.

[7] "documento 16/EN WP 243 "Linee guida sui responsabili della protezione dei dati (RPD)" del WP29 adottate il 13 dicembre 2016. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A.

[8] *"WP29 Opinion 03/2013 on purpose limitation"* [Parere 03/2013 del WP29 sulla limitazione della finalità] - 13/EN WP 203, approvato il 2 aprile 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recom-

mendation/files/2013/wp203en.pdf?wb48617274=39E0E409.

[9] Ad esempio la norma ISO 31000:2009, *Gestione del rischio - Principi e linee guida*, Organizzazione internazionale per la normazione (ISO); ISO/IEC 29134 (progetto), *Information technology – Security techniques – Privacy impact assessment – Guidelines* (in inglese), Organizzazione internazionale per la normazione (ISO).

[10] Va sottolineato che al fine di poter gestire i rischi per i diritti e le libertà delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. I titolari del trattamento non possono sottrarsi alla loro responsabilità coprendo i rischi stipulando polizze assicurative.

[11] Cfr. i considerando 89 e 91 e l'articolo 35, paragrafi 1 e 3, per ulteriori esempi.

[12] Cfr. considerando 71: *"in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali"*.

[13] Cfr. considerando 75: *"se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza"*.

[14] Cfr. ad esempio i considerando 75, 76, 92 e 116.

[15] L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del WP29 (cfr. le "Linee guida sui responsabili della protezione dei dati (RPD)" del WP29 - 16/EN WP 243):
- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Il termine *"zona accessibile al pubblico"*, a giudizio del WP29, indica qualsiasi luogo aperto a ciascun individuo della popolazione, come ad esempio una piazza, un centro commerciale, una strada, un mercato, una stazione ferroviaria o una biblioteca pubblica.

[16] Cfr. "Linee guida sui responsabili della protezione dei dati (RPD)" del WP29 - 16/EN WP 243.

[17] Cfr. spiegazione contenuta nel parere del WP29 sulla limitazione della finalità - 13/EN WP 203, pag. 24.

[18] In tale contesto, *"l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione"* (articolo 35, paragrafo 6).

[19] *"Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi"*.

[20] *"Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate"* (considerando 171).

[21] Quando viene svolta una valutazione d'impatto sulla protezione dei dati in fase di elaborazione della legislazione che fornisce una base giuridica per un trattamento, è probabile che la stessa richieda un riesame prima dell'avvio delle attività, in quanto la legislazione adottata può differire dalla proposta ed influenzare quindi questioni in materia di vita privata e protezione dei dati. Inoltre, potrebbero non esserci sufficienti dettagli tecnici per quanto riguarda il trattamento effettivo al momento dell'adozione della legislazione, anche qualora detto trattamento sia accompagnato da una valutazione d'impatto sulla protezione dei dati. In questi casi, può comunque essere necessario eseguire una valutazione d'impatto sulla protezione dei dati specifica pri-

ma di realizzare le attività di trattamento effettive.

[22] In termini di contesto, i dati raccolti, le finalità, le funzionalità, i dati personali trattati, i destinatari, le combinazioni di dati, i rischi (risorse di sostegno, fonti di rischio, impatti potenziali, minacce, ecc.), le misure di sicurezza e i trasferimenti internazionali.

[23] Fatto salvo il caso in cui si tratti di un trattamento già in essere che è stato preventivamente verificato dall'autorità di controllo, nel qual caso la valutazione d'impatto sulla protezione dei dati deve essere eseguita prima di attuare modifiche significative.

[24] *"Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3"*: http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

[25] Va sottolineato che il processo descritto in questa sede è iterativo: in pratica, è probabile che ciascuna delle fasi venga riesaminata più volte prima che sia possibile completare la valutazione d'impatto sulla protezione dei dati.

[26] Processi di gestione del rischio: comunicazione e consultazione, definizione del contesto, valutazione dei rischi, trattamento dei rischi, monitoraggio e riesame (cfr. termini e definizioni e l'indice nell'anteprima della norma ISO 31000 (in inglese): https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

[27] L'articolo 35, paragrafo 10, esclude esplicitamente soltanto l'applicazione dell'articolo 35, paragrafi da 1 a 7.

[28] La formulazione di un parere scritto a favore del titolare del trattamento è necessaria soltanto quando l'autorità di controllo ritiene che il trattamento previsto non sia conforme al regolamento a norma dell'articolo 36, paragrafo 2.

[29] Tra le quali si annoverano la considerazione degli orientamenti esistenti formulati dal comitato europeo per la protezione dei dati e dalle autorità di controllo, nonché dello stato dell'arte e dei costi di attuazione, come previsto dall'articolo 35, paragrafo 1.

[30] Nota: *"la pseudonimizzazione e la cifratura dei dati personali"* (così come la minimizzazione dei dati, meccanismi di controllo, ecc.) non sono necessariamente misure appropriate. Sono soltanto esempi. Le misure adeguate dipendono dal contesto e dai rischi, aspetti specifici dei trattamenti effettuati.

[31] Approvato all'unanimità e affermativamente (con l'astensione della Baviera) dalla 92a conferenza delle autorità indipendenti per la protezione dei dati del Bund e dei Länder di Kühlungsborn tenutasi il 9 e 10 novembre 2016.

[32] Cfr. anche: Raccomandazione della Commissione, del 12 maggio 2009, sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza. http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32009H0387&from=IT; Parere 9/2011 sulla proposta rivista dell'industria relativa a un quadro per la realizzazione di valutazioni di impatto sulla protezione della vita privata e dei dati per le applicazioni RFID. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_it.pdf.

[33] Cfr. anche il "Parere 07/2013 concernente il modello di valutazione d'impatto sulla protezione dei dati per la rete intelligente e i sistemi di misurazione intelligenti ("modello di valutazione d'impatto sulla protezione dei dati") elaborato dal gruppo di esperti n. 2 della task force della Commissione per le reti intelligenti.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_it.pdf.

[34] ISO/IEC 29134 (progetto), *Information technology – Security techniques – Privacy impact assessment – Guidelines* (in inglese), Organizzazione internazionale per la normazione (ISO).

Linee guida sui responsabili della protezione dei dati [WP 243 rev. 01]

Adottate il 13 dicembre 2016
Versione emendata e adottata in data 5 aprile 2017

IL GRUPPO SULLA TUTELA DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 della stessa,

visto il proprio regolamento,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della Commissione europea, direzione generale Giustizia e consumatori, B -1049 Bruxelles, Belgio, ufficio MO59 05/35.

Sito Internet: http://ec.europa.eu/justice/data-protection/index_en.htm

Indice

7. Si può designare un RPD esterno?
8. Quali sono le qualità professionali che un RPD deve possedere?

Posizione del RPD

9. Quali sono le risorse che titolare del trattamento o responsabile del trattamento dovrebbero mettere a disposizione del RPD?
10. Quali sono le garanzie che possono consentire al RPD di operare con indipendenza? Cosa significa "conflitto di interessi"?

Compiti del RPD

11. Che cosa si intende per "sorvegliare l'osservanza"
12. Il RPD è personalmente responsabile in caso di inosservanza degli obblighi in materia di protezione dei dati?
13. Quale ruolo spetta al RPD con riguardo alla valutazione di impatto sulla protezione dei dati e alla tenuta del registro dei trattamenti?

1. INTRODUZIONE

Il regolamento generale sulla protezione dei dati (RGPD)[1], che esplicherà i propri effetti a partire dal 25 maggio 2018, offre un quadro di riferimento in termini di compliance per la protezione dei dati in Europa, aggiornato e fondato sul principio di responsabilizzazione (accountability). I responsabili della protezione dei dati (RPD) saranno al centro di questo nuovo quadro giuridico in molti ambiti, e saranno chiamati a facilitare l'osservanza delle disposizioni del RGPD.

In base al RGPD, alcuni titolari del trattamento e responsabili del trattamento sono tenuti a nominare un RPD[2]. Ciò vale per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche ovvero trattino su larga scala categorie particolari di dati personali.

Anche ove il regolamento non imponga in modo specifico la designazione di un RPD, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "Articolo 29" (Gruppo di lavoro) incoraggia gli approcci di questo genere.

La figura del RPD non costituisce una novità assoluta. La direttiva 95/46/CE[3] non prevedeva alcun obbligo di nomina di un RPD, ma in molti Stati membri questa è divenuta una prassi nel corso degli anni.

Ancor prima dell'adozione del RGPD, il Gruppo di lavoro ha sostenuto che questa figura rappresenti un elemento fondante ai fini della responsabilizzazione, e che la nomina del RPD possa facilitare l'osservanza della normativa e aumen-

tare il margine competitivo delle imprese[4]. Oltre a favorire l'osservanza attraverso strumenti di accountability (per esempio, supportando valutazioni di impatto e conducendo o supportando audit in materia di protezione dei dati), i RPD fungono da interfaccia fra i soggetti coinvolti: autorità di controllo, interessati, divisioni operative all'interno di un'azienda o di un ente.

I RPD non rispondono personalmente in caso di inosservanza del RGPD. Quest'ultimo chiarisce che spetta al titolare del trattamento o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del regolamento stesso (articolo 24, paragrafo 1). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare del trattamento o sul responsabile del trattamento.

Inoltre, al titolare del trattamento o al responsabile del trattamento spetta il compito fondamentale di consentire lo svolgimento efficace dei compiti cui il RPD è preposto. La nomina di un RPD è solo il primo passo, perché il RPD deve disporre anche di autonomia e risorse sufficienti per svolgere in modo efficace i propri compiti.

Il RGPD riconosce nel RPD uno degli elementi chiave all'interno del nuovo sistema di governance dei dati, e prevede una serie di condizioni in rapporto alla nomina, allo status e ai compiti specifici. Le presenti linee guida intendono fare chiarezza sulle pertinenti disposizioni del regolamento al fine di favorire l'osservanza della normativa da parte di titolari del trattamento e responsabili del trattamento; inoltre, le linee guida vogliono essere di ausilio ai RPD nell'esecuzione dei compiti loro attribuiti. Il presente documento contiene anche alcune raccomandazioni, in termini di migliori prassi, che scaturiscono dall'esperienza accumulata in alcuni Stati membri. Il Gruppo di lavoro monitorerà l'attuazione delle linee guida qui presentate e provvederà alle integrazioni che si riveleranno opportune.

2. NOMINA DI UN RPD

2.1. NOMINA OBBLIGATORIA

In base all'articolo 37, paragrafo 1, del RGPD, la nomina di un RPD è obbligatoria in tre casi specifici[5]:

a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico[6];
b) se le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
c) se le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento su larga scala di categorie particolari di dati[7] o[8] di dati personali relativi a condanne penali e reati[9].

Nelle sottosezioni che seguono, il Gruppo di lavoro fornisce indicazioni sui criteri e sulle formulazioni utilizzati all'articolo 37, paragrafo 1.

Tranne quando sia evidente che un soggetto non è tenuto a nominare un RPD, il Gruppo di lavoro raccomanda a titolari del trattamento e responsabili del trattamento di documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se si applichi o meno l'obbligo di nomina di un RPD, così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti[10]. Tale analisi fa parte della documentazione da produrre in base al principio di responsabilizzazione. Può essere richiesta dall'autorità di controllo e dovrebbe essere aggiornata ove necessario, per esempio se i titolari del trattamento o i responsabili del trattamento intraprendono nuove attività o forniscono nuovi servizi che potrebbero ricadere nel novero dei casi elencati all'articolo 37, paragrafo 1.

Se si procede alla nomina di un RPD su base volontaria, troveranno applicazione tutti i requisiti di cui agli articoli 37-39 per quanto concerne la nomina stessa, lo status e i compiti del RPD esattamente come nel caso di una nomina obbligatoria.

Nulla osta a che un'azienda o un ente, quando non sia soggetta all'obbligo di designare un RPD e non intenda procedere a tale designazione su base volontaria, ricorra comunque a personale o consulenti esterni incaricati di incombenze relative alla protezione dei dati personali. In tal caso è fondamentale garantire che non vi siano ambiguità in termini di denominazione, status e compiti di queste figure; è dunque essenziale che in tutte le comunicazioni interne all'azienda e anche in quelle esterne (con l'autorità di controllo, gli interessati, i soggetti esterni in genere), queste figure o consulenti non siano indicati con la denominazione di responsabile per la protezione dei dati (RPD)[11].

Il RPD viene designato, su base obbligatoria o meno, per tutti i trattamenti svolti dal titolare del trattamento o dal responsabile del trattamento.

2.1.1. "AUTORITÀ PUBBLICA O ORGANISMO PUBBLICO"

Nel regolamento non si rinviene alcuna definizione di "autorità pubblica" o "organismo pubblico". Il Gruppo di lavoro ritiene che tale definizione debba essere conforme al diritto nazionale; conseguentemente, sono autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicabile, la nozione ricomprende anche tutta una serie di altri organismi di diritto pubblico[12]. In questi casi la nomina di un RPD è obbligatoria.

Lo svolgimento di funzioni pubbliche e l'esercizio di pubblici poteri[13] non pertengono esclusivamente alle autorità pubbliche e agli organismi pubblici, potendo riferirsi anche ad altre persone fisiche o giuridiche, di diritto pubblico

o privato, in ambiti che variano a seconda delle disposizioni fissate nel diritto interno di ciascuno Stato membro: trasporti pubblici, forniture idriche ed elettriche, infrastrutture stradali, emittenti radiotelevisive pubbliche, istituti per l'edilizia pubblica o organismi di disciplina professionale.

In tutti questi casi la situazione in cui versano gli interessati è probabilmente molto simile a quella in cui il trattamento è svolto da un'autorità pubblica o da un organismo pubblico. Più in particolare, i trattamenti perseguono finalità simili e spesso il singolo ha, in modo analogo, un margine esiguo o nullo rispetto alla possibilità di decidere se e come possano essere trattati i propri dati personali; pertanto, è verosimile che sia necessaria l'ulteriore tutela offerta dalla nomina di un RPD.

Benché nei casi sopra descritti non sussista l'obbligo di nominare un RPD, il Gruppo di lavoro raccomanda, in termini di buone prassi, che gli organismi privati incaricati di funzioni pubbliche o che esercitano pubblici poteri nominino un RPD. Le attività del RPD nominato nei termini sopra indicati si estendono a tutti i trattamenti svolti, compresi quelli che non sono connessi all'espletamento di funzioni pubbliche o all'esercizio di pubblici poteri quali, per esempio, la gestione di un database del personale.

2.1.2. "ATTIVITÀ PRINCIPALI"

L'articolo 37, paragrafo 1, lettere b) e c), del RGPD contiene un riferimento alle *"attività principali del titolare del trattamento o del responsabile del trattamento"*. Nel considerando 97 si afferma che le attività principali di un titolare del trattamento *"riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria"*. Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento.

Tuttavia, l'espressione "attività principali" non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare del trattamento o dal responsabile del trattamento. Per esempio, l'attività principale di un ospedale consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente. Ne deriva che il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualsiasi ospedale, e che gli ospedali sono tenuti a nominare un RPD.

A titolo di ulteriore esemplificazione, si può citare il caso di un'impresa di sicurezza privata incaricata della sorveglianza di più centri commerciali e aree pubbliche. L'attività principale dell'impresa consiste nella sorveglianza, e questa, a sua volta, è legata in modo inscindibile al trattamento di dati personali. Ne consegue che anche l'impresa in oggetto deve nominare un RPD.

D'altro canto, tutti gli organismi (pubblici e privati) svolgono determinate attività quali il pagamento delle retribuzioni al personale o la predisposizione di strutture standard di supporto informatico. Si tratta di esempi di funzioni di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o essenziali sono considerate solitamente accessorie e non vengono annoverate fra le attività principali.

2.1.3. "LARGA SCALA"

In base all'articolo 37, paragrafo 1, lettere b) e c), del RGPD, occorre che il trattamento di dati personali avvenga su larga scala per far scattare l'obbligo di nomina di un RPD. Nel regolamento non si dà alcuna definizione di trattamento su larga scala, anche se il considerando 91 fornisce indicazioni in proposito[14].

In realtà è impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità; d'altra parte, ciò non significa che sia impossibile, col tempo, individuare alcuni standard utili a specificare in termini più specifici e/o quantitativi cosa debba intendersi per "larga scala" con riguardo ad alcune tipologie di trattamento maggiormente comuni. Anche il Gruppo di lavoro intende contribuire alla definizione di questi standard pubblicando e mettendo a fattor comune esempi delle soglie applicabili per la nomina di un RPD.

A ogni modo, il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Alcuni esempi di trattamento su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile del trattamento specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;

- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Alcuni esempi di trattamento non su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

2.1.4. "MONITORAGGIO REGOLARE E SISTEMATICO"

Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del RGPD; tuttavia, il considerando 24 menziona il "monitoraggio del comportamento di detti interessati"[15] ricomprendendovi senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale.

Occorre rilevare, però, che la nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente online, e che il tracciamento online va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati[16].

L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei pre-

mi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

2.1.5. CATEGORIE PARTICOLARI DI DATI E DATI RELATIVI A CONDANNE PENALI E A REATI

Le disposizioni dell'articolo 37, paragrafo 1, lettera c), riguardano il trattamento di categorie particolari di dati ai sensi dell'articolo 9 e di dati personali relativi a condanne penali e a reati di cui all'articolo 10. Nonostante l'utilizzo della congiunzione "e" nel testo, non vi sono motivazioni sistematiche che impongano l'applicazione simultanea dei due criteri. Pertanto, il testo deve essere interpretato come se recasse la congiunzione "o". [NdT: il testo italiano del regolamento reca già la congiunzione "o"]

2.2. RPD DEL RESPONSABILE DEL TRATTAMENTO

Per quanto riguarda la nomina di un RPD, l'articolo 37 non distingue fra titolari del trattamento[17] e responsabili del trattamento[18] in termini di sua applicabilità. A seconda di chi soddisfi i criteri relativi all'obbligatorietà della nomina, potrà essere il solo titolare del trattamento ovvero il solo responsabile del trattamento, oppure sia l'uno sia l'altro a dover nominare un RPD; questi ultimi saranno poi tenuti alla reciproca collaborazione.

Vale la pena di evidenziare che anche qualora il titolare del trattamento sia tenuto, in base ai criteri suddetti, a nominare un RPD, il suo eventuale responsabile del trattamento non è detto sia egualmente tenuto a procedere a tale nomina – che però può costituire una buona prassi.

Alcuni esempi:

- Una piccola azienda a conduzione familiare operante nel settore della distribuzione di elettrodomestici in una città si serve di un responsabile del trattamento la cui attività principale consiste nel fornire servizi di tracciamento degli utenti del sito web oltre all'assistenza per attività di pubblicità e marketing mirati. Le attività svolte dall'azienda e dai clienti non generano trattamenti di dati "su larga scala", in considerazione del ridotto numero di clienti e della gamma relativamente limitata di attività. Tuttavia, il responsabile del trattamento, che conta numerosi clienti come questa piccola azienda familiare, svolge, nel suo complesso, trattamenti su larga scala. Ne deriva che il responsabile del trattamento deve nominare un RPD ai sensi dell'articolo 37, paragrafo 1, lettera b); al con-

tempo, l'azienda in quanto tale non è soggetta all'obbligo di nomina del RPD.

- Un'azienda di medie dimensioni che produce rivestimenti in ceramica incarica un responsabile esterno della gestione dei servizi di salute occupazionale; tale responsabile ha un numero elevato di clienti con caratteristiche analoghe. Il responsabile del trattamento è tenuto a nominare un RPD ai sensi dell'articolo 37, paragrafo 1, lettera b), poiché svolge trattamenti su larga scala. Tuttavia, l'azienda non è tenuta necessariamente allo stesso adempimento.

Il RPD nominato da un soggetto responsabile del trattamento vigila anche sulle attività svolte da tale soggetto quando operi in qualità di autonomo titolare del trattamento – per esempio, rispetto ai dati concernenti il personale, le risorse informatiche, la logistica.

2.3. DESIGNAZIONE DI UN UNICO RPD PER PIÙ ORGANISMI

L'articolo 37, paragrafo 2, consente a un gruppo imprenditoriale di nominare un unico RPD a condizione che quest'ultimo sia "facilmente raggiungibile da ciascuno stabilimento". Il concetto di raggiungibilità si riferisce ai compiti del RPD in quanto punto di contatto per gli interessati[19], l'autorità di controllo[20] e i soggetti interni all'organismo o all'ente, visto che uno dei compiti del RPD consiste nell' *"informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento"*[21].

Allo scopo di assicurare la raggiungibilità del RPD, interno o esterno, è importante garantire la disponibilità dei dati di contatto nei termini previsti dal RGPD[22].

Il RPD, se necessario con il supporto di un team di collaboratori, deve essere in grado di comunicare con gli interessati[23] in modo efficiente e di collaborare[24] con le autorità di controllo interessate. Ciò significa, fra l'altro, che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa. Il fatto che il RPD sia raggiungibile – vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione – è fondamentale al fine di garantire all'interessato la possibilità di contattare il RPD stesso.

Ai sensi dell'articolo 37, paragrafo 3, è ammessa la designazione di un unico RPD per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione. Valgono le stesse considerazioni svolte in tema di risorse e comunicazioni. Poiché il RPD è chiamato a una molteplicità di funzioni, il titolare del trattamento o il responsabile del trattamento deve assicurarsi che un unico RPD, se necessario supportato da un team di colla-

boratori, sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici.

2.4. ACCESSIBILITÀ E LOCALIZZAZIONE DEL RPD

Ai sensi dell'articolo 4 [sic] del RGPD, l'accessibilità del RPD deve essere effettivamente tale. Per garantire tale accessibilità, il Gruppo di lavoro raccomanda che il RPD sia localizzato nel territorio dell'Unione europea, indipendentemente dal fatto che il titolare del trattamento o il responsabile del trattamento siano stabiliti nell'UE.

Tuttavia, non si può escludere che, in alcuni casi ove il titolare del trattamento o il responsabile del trattamento non sono stabiliti nell'UE[25], un RPD sia in grado di svolgere i propri compiti con maggiore efficacia operando al di fuori del territorio dell'UE.

2.5. CONOSCENZE E COMPETENZE DEL RPD

In base all'articolo 37, paragrafo 5, il RPD *"è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39"*. Nel considerando 97 si prevede che il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento.

- **Conoscenze specialistiche**

Il livello di conoscenza specialistica richiesto non trova una definizione tassativa; piuttosto, deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento. Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il RPD avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto. Occorre anche distinguere in base all'esistenza di trasferimenti sistematici ovvero occasionali di dati personali al di fuori dell'Unione europea. Ne consegue la necessità di una particolare attenzione nella scelta del RPD, in cui si tenga adeguatamente conto delle problematiche in materia di protezione dei dati con cui il singolo titolare deve confrontarsi.

- **Qualità professionali**

L'articolo 37, paragrafo 5, non specifica le qualità professionali da prendere in considerazione nella nomina di un RPD; tuttavia, sono pertinenti al riguardo la conoscenza da parte del RPD della normativa e delle prassi nazionali ed europee in materia di protezione dei dati e un'approfondita conoscenza del RGPD.

Proficua anche la promozione di una formazione adeguata e continua rivolta ai RPD da parte delle Autorità di controllo.

E' utile la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare del trattamento; inoltre, il RPD dovrebbe avere buona familiarità con le operazioni di trattamento svolte nonché con i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal titolare.

Nel caso di un'autorità pubblica o di un organismo pubblico, il RPD dovrebbe possedere anche una conoscenza approfondita delle norme e procedure amministrative applicabili.

- **Capacità di assolvere i propri compiti**

Per capacità di assolvere i propri compiti si deve intendere sia quanto è legato alle qualità personali e alle conoscenze del RPD, sia quanto dipende dalla posizione del RPD all'interno dell'azienda o dell'organismo. Le qualità personali dovrebbero comprendere, per esempio, l'integrità ed elevati standard deontologici; il RPD dovrebbe perseguire in via primaria l'osservanza delle disposizioni del RGPD. Il RPD svolge un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'azienda o dell'organismo, e contribuisce a dare attuazione a elementi essenziali del regolamento quali i principi fondamentali del trattamento[26], i diritti degli interessati[27], la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita[28], i registri delle attività di trattamento[29], la sicurezza dei trattamenti[30] e la notifica e comunicazione delle violazioni di dati personali[31].

- **RPD sulla base di un contratto di servizi**

La funzione di RPD può essere esercitata anche in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna all'organismo o all'azienda titolare/responsabile del trattamento. In tal caso, è indispensabile che ciascun soggetto appartenente alla persona giuridica e operante quale RPD soddisfi tutti i requisiti applicabili come fissati nella Sezione 4 del RGPD; per esempio, è indispensabile che nessuno di tali soggetti versi in situazioni di conflitto di interessi. Pari importanza riveste il fatto che ciascuno dei soggetti in questione goda delle tutele previste dal RGPD: per esempio, non è ammissibile la risoluzione ingiustificata del contratto di servizi in rapporto alle attività svolte in quanto RPD, né è ammissibile l'ingiustificata rimozione di un singolo appartenente alla persona giuridica che svolga funzioni di RPD. Al contempo, si potranno associare le competenze e le capacità individuali affinché il contributo collettivo fornito da più soggetti consenta di rendere alla clientela un servizio più efficiente.

Per favorire una corretta e trasparente organizzazione interna e prevenire conflitti di interesse a carico dei componenti il *team* RPD, si raccomanda di procedere a una chiara ripartizione dei compiti all'interno del *team* RPD e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato"

per ciascun cliente. Sarà utile, in via generale, inserire specifiche disposizioni in merito nel contratto di servizi.

2.6. PUBBLICAZIONE E COMUNICAZIONE DEI DATI DI CONTATTO DEL RPD

L'articolo 37, settimo paragrafo, del RGPD impone al titolare del trattamento o al responsabile del trattamento

- di pubblicare i dati di contatto del RPD, e
- di comunicare i dati di contatto del RPD alle pertinenti autorità di controllo.

Queste disposizioni mirano a garantire che tanto gli interessati (all'interno o all'esterno dell'ente/organismo titolare o responsabile del trattamento) quanto le autorità di controllo possano contattare il RPD in modo facile e diretto senza doversi rivolgere a un'altra struttura operante presso il titolare/responsabile del trattamento. Anche la confidenzialità riveste pari importanza; per esempio, i dipendenti possono essere riluttanti a presentare reclami al RPD se non viene garantita la confidenzialità delle loro comunicazioni. Il RPD è tenuto a osservare le norme in materia di segreto o confidenzialità nello svolgimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri (articolo 38, paragrafo 5).

I dati di contatto del RPD dovrebbero comprendere tutte le informazioni che consentono agli interessati e all'autorità di controllo di raggiungere facilmente il RPD stesso: recapito postale, numero telefonico dedicato e/o indirizzo dedicato di posta elettronica. Se opportuno, per facilitare la comunicazione con il pubblico, si potrebbero indicare anche canali ulteriori: una hotline dedicata, un modulo specifico per contattare il RPD pubblicato sul sito del titolare/responsabile del trattamento.

In base all'articolo 37, settimo paragrafo, del RGPD non è necessario pubblicare anche il nominativo del RPD. Seppure ciò rappresenti con ogni probabilità di una buona prassi, spetta al titolare del trattamento o al responsabile del trattamento e allo stesso RPD stabilire se si tratti di un'informazione necessaria o utile nelle specifiche circostanze[32]. Tuttavia, comunicare il nominativo del RPD all'autorità di controllo è fondamentale affinché il RPD funga da punto di contatto fra il singolo ente o organismo e l'autorità di controllo stessa (articolo 39, paragrafo 1, lettera e)).

In termini di buone prassi, il Gruppo di lavoro raccomanda, inoltre, che il titolare/responsabile del trattamento comunichi ai dipendenti il nominativo e i dati di contatto del RPD. Per esempio, queste informazioni (nominativo e dati di contatto) potrebbero essere pubblicate sulla intranet del titolare/responsabile del trattamento, inserite nell'elenco telefonico interno e nei diversi organigrammi della struttura.

3. POSIZIONE DEL RPD

3.1. COINVOLGIMENTO DEL RPD IN TUTTE LE QUESTIONI RIGUARDANTI LA PROTEZIONE DEI DATI PERSONALI

Ai sensi dell'articolo 38 del RGPD, il titolare del trattamento e il responsabile del trattamento assicurano che il RPD sia *"tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali"*.

E' essenziale che il RPD, o il suo team di collaboratori, sia coinvolto quanto prima possibile in ogni questione attinente la protezione dei dati. Per quanto concerne le valutazioni di impatto sulla protezione dei dati, il regolamento prevede espressamente che il RPD vi sia coinvolto fin dalle fasi iniziali e specifica che il titolare del trattamento ha l'obbligo di consultarlo nell'effettuazione di tali valutazioni[33]. Assicurare il tempestivo e immediato coinvolgimento del RPD, tramite la sua informazione e consultazione fin dalle fasi iniziali, faciliterà l'osservanza del RGPD e promuoverà l'applicazione del principio di privacy (e protezione dati) fin dalla fase di progettazione; pertanto, questo dovrebbe rappresentare l'approccio standard all'interno della struttura del titolare/responsabile del trattamento. Inoltre, è importante che il RPD sia annoverato fra gli interlocutori all'interno della struttura suddetta, e che partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento.

Ciò significa che occorrerà garantire, per esempio:

- che il RPD sia invitato a partecipare su base regolare alle riunioni del management di alto e medio livello;
- la presenza del RPD ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati. Il RPD deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza idonea;
- che il parere del RPD riceva sempre la dovuta considerazione. In caso di disaccordi, il Gruppo di lavoro raccomanda, quale buona prassi, di documentare le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal RPD;
- che il RPD sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

Ove opportuno, il titolare del trattamento o il responsabile del trattamento potrebbero mettere a punto linee guida ovvero programmazioni in materia di protezione dei dati che indichino i casi di consultazione obbligatoria del RPD.

3.2. RISORSE NECESSARIE

L'articolo 38, paragrafo 2, del RGPD obbliga il titolare del trattamento o il responsabile del trattamento a sostenere il RPD *"fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere*

la propria conoscenza specialistica". Ciò si traduce, in modo particolare, nelle indicazioni seguenti:

- supporto attivo delle funzioni del RPD da parte del senior management (per esempio, a livello del consiglio di amministrazione);
- tempo sufficiente per l'espletamento dei compiti affidati al RPD. Ciò riveste particolare importanza se viene designato un RPD interno con un contratto part-time, oppure se il RPD esterno si occupa di protezione dati oltre a svolgere altre incombenze. In caso contrario, il rischio è che le attività cui il RPD è chiamato finiscano per essere trascurate a causa di conflitti con altre priorità. E' fondamentale disporre di tempo sufficiente da dedicare allo svolgimento dei compiti previsti per il RPD; una prassi da raccomandare consiste nel definire la percentuale del tempo lavorativo destinata alle attività di RPD quando quest'ultimo svolga anche altre funzioni. Un'altra buona prassi consiste nello stabilire il tempo necessario per adempiere alle relative incombenze, definire il livello di priorità spettante a tale incombenze, e prevedere che il RPD stesso (ovvero l'azienda/l'organismo titolare o responsabile) rediga un piano di lavoro;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;
- comunicazione ufficiale della nomina del RPD a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'azienda/dell'organismo;
- accesso garantito ad altri servizi (risorse umane, ufficio giuridico, IT, sicurezza, ecc.) così da fornire al RPD supporto, informazioni e input essenziali;
- formazione permanente. I RPD devono avere la possibilità di curare il proprio aggiornamento con riguardo agli sviluppi nel settore della protezione dati. Ciò mira, in ultima analisi, a consentire un incremento continuo del livello di competenze proprio dei RPD, che dovrebbero essere incoraggiati a partecipare a corsi di formazione su materie attinenti alla protezione dei dati e ad altre occasioni di professionalizzazione (forum in materia di privacy, workshop, ecc.);
- alla luce delle dimensioni e della struttura della singola azienda/del singolo organismo, può risultare necessario costituire un ufficio o un gruppo di lavoro RPD (formato dal RPD stesso e dal rispettivo personale). In casi del genere, è opportuno definire con precisione la struttura interna del gruppo di lavoro nonché i compiti e le responsabilità individuali. Analogamente, se la funzione di RPD viene esercitata da un fornitore di servizi esterno all'azienda/all'organismo, potrà aversi la costituzione di un gruppo di lavoro formato da soggetti operanti per conto di tale fornitore e incaricati di svolgere le funzioni di RPD sotto la direzione di un responsabile che funga da contatto per il cliente.

In linea di principio, quanto più aumentano complessità e/o sensibilità dei trattamenti, tanto maggiori devono essere le risorse messe a disposizione del RPD. La funzione "protezione dati" deve poter operare con efficienza e contare su risorse sufficienti in proporzione al trattamento svolto.

3.3. ISTRUZIONI E [SIGNIFICATO DI] "ADEMPIERE ALLE FUNZIONI E AI COMPITI LORO INCOMBENTI IN MANIERA INDIPENDENTE"

L'articolo 38, paragrafo 3, fissa alcune garanzie essenziali per consentire ai RPD di operare con un grado sufficiente di autonomia all'interno dell'organizzazione del titolare/responsabile del trattamento. In particolare, questi ultimi sono tenuti ad assicurare che il RPD *"non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti"*. Il considerando 97 aggiunge che i RPD *"dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente"*.

Ciò significa che il RPD, nell'esecuzione dei compiti attribuitigli ai sensi dell'articolo 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico – quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo. Né deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Tuttavia, l'autonomia del RPD non significa che quest'ultimo disponga di un margine decisionale superiore al perimetro dei compiti fissati nell'articolo 39.

Il titolare del trattamento o il responsabile del trattamento mantengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado di dimostrare tale osservanza[34]. Se il titolare del trattamento o il responsabile del trattamento assumono decisioni incompatibili con il RGPD e le indicazioni fornite dal RPD, quest'ultimo dovrebbe avere la possibilità di manifestare il proprio dissenso al più alto livello del management e ai decisori. Al riguardo, l'articolo 38, paragrafo 3, prevede che il RPD "riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento". Tale rapporto diretto garantisce che il vertice amministrativo (per esempio, il consiglio di amministrazione) sia a conoscenza delle indicazioni e delle raccomandazioni fornite dal RPD nel quadro della sue funzioni di informazione e consulenza a favore del titolare del trattamento o del responsabile del trattamento. Un altro esempio di tale rapporto diretto consiste nella redazione di una relazione annuale delle attività svolte dal RPD da sottoporre al vertice gerarchico.

3.4. RIMOZIONE O PENALIZZAZIONI IN RAPPORTO ALL'ADEMPIMENTO DEI COMPITI DI RPD

L'articolo 38, paragrafo 3, prevede che il RPD *"non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti"*.

Questa prescrizione mira a potenziare l'autonomia del RPD e ad assicurarne l'indipendenza nell'adempimento dei compiti assegnatigli, attraverso la previsione di un'adeguata tutela.

Il divieto di penalizzazioni menzionato nel RGPD si applica solo con riguardo a quelle penalizzazioni eventualmente derivanti dallo svolgimento dei compiti propri del RPD. Per esempio, un RPD può ritenere che un determinato trattamento comporti un rischio elevato e quindi raccomandare al titolare del trattamento o al responsabile del trattamento di condurre una valutazione di impatto, ma questi ultimi non concordano con la valutazione del RPD. In casi del genere non è ammissibile che il RPD sia rimosso dall'incarico per avere formulato la raccomandazione in oggetto.

Le penalizzazioni possono assumere molte forme e avere natura diretta o indiretta. Per esempio, potrebbero consistere nella mancata o ritardata promozione, nel blocco delle progressioni di carriera, nella mancata concessione di incentivi rispetto ad altri dipendenti. Non è necessario che si arrivi all'effettiva applicazione di una penalizzazione, essendo sufficiente anche la sola minaccia nella misura in cui sia rivolta al RPD in rapporto alle attività da questi svolte.

Viceversa, e conformemente alle normali regole di gestione applicabili a ogni altro dipendente o fornitore soggetto alla disciplina del rispettivo contratto nazionale ovvero alle norme di diritto penale e del lavoro, sarebbe legittimamente possibile interrompere il rapporto con il RPD per motivazioni diverse dallo svolgimento dei compiti che gli sono propri: per esempio, in caso di furto, molestie sessuali o di altro genere, o altre analoghe e gravi violazioni deontologiche.

In questo ambito va rilevato che il RGPD non specifica le modalità e la tempistica riferite alla cessazione del rapporto di lavoro del RPD o alla sua sostituzione. Tuttavia, quanto maggiore è la stabilità del contratto stipulato con il RPD e maggiori le tutele previste contro l'ingiusto licenziamento, tanto maggiore sarà la probabilità che l'azione del RPD si svolga in modo indipendente. Il Gruppo di lavoro vede, quindi, con favore ogni iniziativa assunta in tal senso dai titolari del trattamento e responsabili del trattamento.

3.5. CONFLITTO DI INTERESSI

In base all'articolo 38, paragrafo 6, al RPD è consentito di *"svolgere altri compiti e funzioni"*, ma a condizione che il titolare del trattamento o il responsabile del trattamento si assicuri che *"tali compiti e funzioni non diano adito a un conflitto di interessi"*.

L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza. Anche se un RPD può svolgere altre funzioni, l'affidamento di tali ulteriori compiti e funzioni è possibile solo a condizione che essi non diano adito a conflitti di interessi. Ciò significa, in modo particolare, che un RPD non può rivestire, all'interno dell'organizzazione del titolare del trattamento o del responsabile del trattamento, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali. Si tratta di un elemento da tenere in

considerazione caso per caso guardando alla specifica struttura organizzativa del singolo titolare del trattamento o responsabile del trattamento.

A grandi linee, possono sussistere situazioni di conflitto all'interno dell'organizzazione del titolare del trattamento o del responsabile del trattamento riguardo a ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento. Inoltre, può insorgere un conflitto di interessi se, per esempio, a un RPD esterno si chiede di rappresentare il titolare o il responsabile in un giudizio che tocchi problematiche di protezione dei dati.

A seconda delle attività, delle dimensioni e della struttura organizzativa del titolare del trattamento o del responsabile del trattamento, si possono indicare le seguenti buone prassi:

- individuare le qualifiche e funzioni che sarebbero incompatibili con quella di RPD;
- redigere regole interne a tale scopo onde evitare conflitti di interessi;
- prevedere un'illustrazione più articolata dei casi di conflitto di interessi;
- dichiarare che il RPD non versa in alcuna situazione di conflitto di interessi con riguardo alle funzioni di RPD, al fine di sensibilizzare rispetto al requisito in questione;
- prevedere specifiche garanzie nelle regole interne e fare in modo che nel segnalare la disponibilità di una posizione lavorativa quale RPD ovvero nel redigere il contratto di servizi si utilizzino formulazioni sufficientemente precise e dettagliate così da prevenire conflitti di interessi. Al riguardo, si deve ricordare, inoltre, che un conflitto di interessi può assumere varie configurazioni a seconda che il RPD sia designato fra soggetti interni o esterni all'organizzazione.

4. COMPITI DEL RPD

4.1. SORVEGLIARE L'OSSERVANZA DEL RGPD

L'articolo 39, paragrafo 1, lettera b), affida al RPD, fra gli altri, il compito di sorvegliare l'osservanza del RGPD. Nel considerando 97 si specifica che il titolare del trattamento o il responsabile del trattamento dovrebbe essere *"assistito [dal RPD] nel controllo del rispetto a livello interno del presente regolamento"*.

Fanno parte di questi compiti di controllo svolti dal RPD, in particolare,

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità,
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

Il controllo del rispetto del regolamento non significa che il RPD sia personalmente responsabile in caso di inosservanza. Il RGPD chiarisce che spetta al titolare, e non al RPD, *"mette[re] in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento"* (articolo 24, paragrafo 1). Il rispetto delle norme in materia di protezione dei dati fa parte della responsabilità d'impresa del titolare del trattamento, non del RPD.

4.2. IL RUOLO DEL RPD NELLA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

In base all'articolo 35, paragrafo 1, spetta al titolare del trattamento, e non al RPD, condurre, ove necessario, una valutazione di impatto sulla protezione dei dati (DPIA, nell'acronimo inglese). Tuttavia, il RPD svolge un ruolo fondamentale e di grande utilità assistendo il titolare nello svolgimento di tale DPIA. In ossequio al principio di "protezione dei dati fin dalla fase di progettazione" (o *data protection by design*), l'articolo 35, paragrafo 2, prevede in modo specifico che il titolare *"si consulta"* con il RPD quando svolge una DPIA. A sua volta, l'articolo 39, paragrafo 1, lettera c) affida al RPD il compito di *"fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35"*.

Il Gruppo di lavoro raccomanda che il titolare del trattamento si consulti con il RPD, fra l'altro, sulle seguenti tematiche[35]:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD.

Qualora il titolare del trattamento non concordi con le indicazioni fornite dal RPD, è necessario che la documentazione relativa alla DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni[36].

Inoltre, il Gruppo di lavoro raccomanda che il titolare del trattamento definisca con chiarezza, per esempio nel contratto stipulato con il RPD, ma anche fornendo informative ai dipendenti, agli amministratori e, ove pertinente, ad altri aventi causa, i compiti specificamente affidati al RPD e i rispettivi ambiti, con particolare riguardo alla conduzione della DPIA.

4.3. COOPERAZIONE CON L'AUTORITÀ DI CONTROLLO E FUNZIONE DI PUNTO DI CONTATTO

In base all'articolo 39, paragrafo 1, lettere d) ed e), il RPD deve "cooperare con l'autorità di controllo" e "fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione".

Questi compiti attengono al ruolo di "facilitatore" attribuito al RPD e già menzionato nell'introduzione alle presenti linee guida. Il RPD funge da punto di contatto per facilitare l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei compiti attribuitile dall'articolo 57 nonché ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi di cui all'articolo 58. Si è già rilevato che il RPD è tenuto al rispetto delle norme in materia di segreto o riservatezza, in conformità del diritto dell'Unione o degli Stati membri (articolo 38, paragrafo 5); tuttavia, tali vincoli di segreto/riservatezza non precludono la possibilità per il RPD di contattare e chiedere lumi all'autorità di controllo. L'articolo 39, paragrafo 1, prevede che il RPD possa consultare l'autorità di controllo con riguardo a qualsiasi altra questione, se del caso.

4.4. APPROCCIO BASATO SUL RISCHIO

In base all'articolo 39, paragrafo 2, il RPD deve *"considera[re] debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo"*.

Si tratta di una disposizione di portata generale e ispirata a criteri di buon senso, verosimilmente applicabile sotto molti riguardi all'attività quotidiana del RPD. In sostanza, si chiede al RPD di definire un ordine di priorità nell'attività svolta e di concentrarsi sulle questioni che presentino maggiori rischi in termini di protezione dei dati. Seppure ciò non significhi che il RPD debba trascurare di sorvegliare il grado di conformità di altri trattamenti associati a un livello di rischio comparativamente inferiore, di fatto la disposizione segnala l'opportunità di dedicare attenzione prioritaria agli ambiti che presentino rischi più elevati.

Attraverso questo approccio selettivo e pragmatico, il RPD dovrebbe essere più facilmente in grado di consigliare al titolare quale metodologia seguire nel condurre una DPIA, a quali settori riservare un audit interno o esterno in tema di protezione dei dati, quali attività di formazione interna prevedere per il personale o gli amministratori che trattino dati personali, e a quali trattamenti dedicare maggiori risorse e tempo.

4.5. IL RUOLO DEL RPD NELLA TENUTA DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

L'articolo 30, primo e paragrafo 2, prevede che sia il titolare del trattamento o il responsabile del trattamento, e non il RPD, a *"ten[ere] un registro delle attività di trattamento svolte sotto la propria responsabilità"* ovvero *"un registro di tutte le categorie di trattamento svolte per conto di un titolare del trattamento"*.

Nella realtà, sono spesso i RPD a realizzare l'inventario dei trattamenti e tenere un registro di tali trattamenti sulla base delle informazioni fornite loro dai vari uffici o unità che trattano dati personali. È una prassi consolidata e fondata sulle disposizioni di numerose leggi nazionali nonché sulla normativa in materia di protezione dati applicabile alle istituzioni e agli organismi dell'UE[37].

L'articolo 39, paragrafo 1, contiene un elenco non esaustivo dei compiti affidati al RPD. Pertanto, niente vieta al titolare del trattamento o al responsabile del trattamento di affidare al RPD il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso. Tale registro va considerato uno degli strumenti che consentono al RPD di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare del trattamento o del responsabile del trattamento.

In ogni caso, il registro la cui tenuta è obbligatoria ai sensi dell'articolo 30 deve essere considerato anche uno strumento che consente al titolare del trattamento e all'autorità di controllo, su richiesta, di disporre di un quadro complessivo dei trattamenti di dati personali svolti dallo specifico soggetto. In quanto tale, esso costituisce un presupposto indispensabile ai fini dell'osservanza delle norme e, pertanto, un'efficace misura di responsabilizzazione.

ALLEGATO ALLE LINEE GUIDA SUL RPD - INDICAZIONI ESSENZIALI

L'allegato intende rispondere, in forma sintetica e semplificata, ad alcune delle domande fondamentali rispetto al nuovo obbligo di designazione di un RPD fissato nel regolamento generale sulla protezione dei dati

Designazione del RPD

1. CHI È TENUTO A DESIGNARE UN RPD?

La designazione di un RPD è obbligatoria:

- se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
- se le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
- se le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Si tenga presente che la designazione obbligatoria di un RPD può essere prevista anche in casi ulteriori in base alla legge nazionale o al diritto dell'UE. Inoltre, anche ove la designazione di un RPD non sia obbligatoria, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "Articolo 29" (Gruppo di lavoro) incoraggia un approccio di questo genere. Qualora si proceda alla designazione di un RPD su base volontaria, si applicano gli identici requisiti - in termini di criteri per la designazione, posizione e compiti - che valgono per i RPD designati in via obbligatoria.

Fonte: articolo 37(1) RGPD

2. COSA SIGNIFICA "ATTIVITÀ PRINCIPALI"?

Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento, comprese tutte quelle attività per le quali il trattamento dei dati è inscindibilmente connesso all'attività del titolare del trattamento o del responsabile del trattamento. Per esempio, il trattamento di dati relativi alla salute (come le cartelle sanitarie dei pazienti) è da ritenersi una delle attività principali di qualsiasi ospedale; ne deriva che tutti gli ospedali dovranno designare un RPD.

D'altra parte, tutti gli organismi (pubblici e privati) svolgono determinate attività quali il pagamento delle retribuzioni al personale ovvero dispongono di strutture standard di supporto informatico. Si tratta di esempi di funzioni

di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o perfino essenziali sono considerate solitamente di natura accessoria e non vengono annoverate fra le attività principali.

Fonte: articolo 37, paragrafo 1, lettere b) e c) RGPD

3. COSA SIGNIFICA "SU LARGA SCALA"?

Il regolamento non definisce cosa rappresenti un trattamento "su larga scala". Il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori qui elencati al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Alcuni esempi di trattamento su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Alcuni esempi di trattamento non su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Fonte: articolo 37, paragrafo 1, lettere b) e c), RGPD

4. COSA SIGNIFICA "MONITORAGGIO REGOLARE E SISTEMATICO"?

Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del RGPD; tuttavia, esso comprende senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale. Non si tratta, però, di un concetto riferito esclusivamente all'ambiente online.

Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Fonte: articolo 37, paragrafo 1, lettera b), RGPD

5. E' AMMESSA LA DESIGNAZIONE CONGIUNTA DI UNO STESSO RPD DA PARTE DI PIÙ SOGGETTI? E A QUALI CONDIZIONI?

Sì. Un gruppo imprenditoriale può nominare un unico RPD a condizione che quest'ultimo sia *"facilmente raggiungibile da ciascuno stabilimento"*. Il concetto di raggiungibilità si riferisce ai compiti del RPD in quanto punto di contatto per gli interessati, l'autorità di controllo e i soggetti interni all'organismo o all'ente. Allo scopo di assicurare la raggiungibilità del RPD, interno o esterno, è importante garantire la disponibilità dei dati di contatto nei termini previsti dal

RGPD. Il RPD, supportato da un apposito *team* se necessario, deve essere in grado di comunicare con gli interessati in modo efficiente e di collaborare con le autorità di controllo interessate. Ciò significa che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa. Il fatto che il RPD sia raggiungibile – vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione – è fondamentale al fine di garantire all'interessato la possibilità di contattare il RPD stesso.

È ammessa la designazione di un unico RPD per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione. Valgono le stesse considerazioni svolte in tema di risorse e comunicazioni. Poiché il RPD è chiamato a una molteplicità di funzioni, il titolare del trattamento o il responsabile del trattamento deve assicurarsi che un unico RPD, se necessario supportato da un team di collaboratori, sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici.

Fonte: articolo 37, paragrafi 2) e 3), RGPD

6. DOVE DOVREBBE COLLOCARSI IL RPD?

Per garantire l'accessibilità del RPD, il Gruppo di lavoro raccomanda la sua collocazione nel territorio dell'Unione europea, indipendentemente dall'esistenza di uno stabilimento del titolare o del responsabile nell'UE. Tuttavia, non si può escludere che un RPD sia in grado di adempiere ai propri compiti con maggiore efficacia operando al di fuori dell'UE in alcuni casi ove titolare del trattamento o responsabile del trattamento non sono stabiliti nel territorio dell'Unione europea.

7. SI PUÒ DESIGNARE UN RPD ESTERNO?

Sì. Il RPD può far parte del personale del titolare del trattamento o del responsabile del trattamento (RPD interno) ovvero *"assolvere i suoi compiti in base a un contratto di servizi"*. In quest'ultimo caso il RPD sarà esterno e le sue funzioni saranno esercitate sulla base di un contratto di servizi stipulato con una persona fisica o giuridica.

Se la funzione di RPD è svolta da un fornitore esterno di servizi, i compiti stabiliti per il RPD potranno essere assolti efficacemente da un *team* operante sotto l'autorità di un contatto principale designato e "responsabile" per il singolo cliente. In tal caso, è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale RPD soddisfi tutti i requisiti applicabili come fissati nel RGPD.

Per favorire efficienza e correttezza e prevenire conflitti di interesse a carico

dei componenti il *team*, le linee guida raccomandano di procedere a una chiara ripartizione dei compiti nel *team* del RPD esterno, attraverso il contratto di servizi, e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente.

Fonte: articolo 37, paragrafo 6, RGPD

8. QUALI SONO LE QUALITÀ PROFESSIONALI CHE UN RPD DEVE POSSEDERE?

Il RPD *"è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i [rispettivi] compiti"*.

Il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento. Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il RPD avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto.

Fra le competenze e conoscenze specialistiche pertinenti rientrano le seguenti:

- conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, compresa un'approfondita conoscenza del RGPD;
- familiarità con le operazioni di trattamento svolte;
- familiarità con tecnologie informatiche e misure di sicurezza dei dati;
- conoscenza dello specifico settore di attività e dell'organizzazione del titolare/del responsabile;
- capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione del titolare/del responsabile.

Fonte: articolo 37, paragrafo 5, RGPD

Posizione del RPD

9. QUALI SONO LE RISORSE CHE TITOLARE DEL TRATTAMENTO O RESPONSABILE DEL TRATTAMENTO DOVREBBERO METTERE A DISPOSIZIONE DEL RPD?

Il RPD deve disporre delle risorse necessarie per assolvere i propri compiti.

A seconda della natura dei trattamenti, e delle attività e dimensioni della struttura del titolare del trattamento o del responsabile del trattamento, il RPD dovrebbe poter contare sulle seguenti risorse:

- supporto attivo della funzione di RPD da parte del *senior management*;
- tempo sufficiente per l'espletamento dei compiti affidati;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;
- comunicazione ufficiale della designazione del RPD a tutto il personale;
- accesso garantito ad altri servizi all'interno della struttura del titolare/del responsabile del trattamento in modo da ricevere tutto il supporto, le informazioni o gli input necessari;
- formazione permanente.

Fonte: articolo 38, paragrafo 2, RGPD

10. QUALI SONO LE GARANZIE CHE POSSONO CONSENTIRE AL RPD DI OPERARE CON INDIPENDENZA? COSA SIGNIFICA "CONFLITTO DI INTERESSI"?

Vi sono numerose garanzie che possono consentire al RPD di operare in modo indipendente:

- nessuna istruzione da parte del titolare del trattamento o del responsabile del trattamento per quanto riguarda lo svolgimento dei compiti affidati al RPD;
- nessuna penalizzazione o rimozione dall'incarico in rapporto allo svolgimento dei compiti affidati al RPD;
- nessun conflitto di interessi con eventuali ulteriori compiti e funzioni.

Gli "altri compiti e funzioni" del RPD non devono comportare conflitti di interessi. Ciò significa, in primo luogo, che il RPD non può rivestire, all'interno dell'organizzazione del titolare del trattamento o del responsabile del trattamento, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali. Si tratta di un elemento da tenere in considerazione caso per caso guardando alla specifica struttura organizzativa del singolo titolare del trattamento o responsabile del trattamento.

A grandi linee, possono sussistere situazioni di conflitto all'interno dell'organizzazione con riguardo a ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento. Inoltre, può insorgere un conflitto di interessi se, per esempio, a un RPD esterno si chiede di rappresentare il titolare del trattamento o il responsabile del trattamento in un giudizio che tocchi problematiche di protezione dei dati.

Fonte: articolo 38, paragrafi 3 e 6, RGPD

11. CHE COSA SI INTENDE PER "SORVEGLIARE L'OSSERVANZA"

Fanno parte di questi compiti di controllo del RPD, in particolare,

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità, e
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare del trattamento o responsabile del trattamento.

Fonte: articolo 39, paragrafo 1, lettera b), RGPD

12. IL RPD È PERSONALMENTE RESPONSABILE IN CASO DI INOSSERVANZA DEGLI OBBLIGHI IN MATERIA DI PROTEZIONE DEI DATI?

No, il RPD non è responsabile personalmente in caso di inosservanza degli obblighi in materia di protezione dei dati. Spetta al titolare del trattamento o al responsabile del trattamento garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento. La responsabilità di garantire l'osservanza della normativa in materia di protezione dei dati ricade sul titolare del trattamento o sul responsabile del trattamento.

13. QUALE RUOLO SPETTA AL RPD CON RIGUARDO ALLA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI E ALLA TENUTA DEL REGISTRO DEI TRATTAMENTI?

Per quanto concerne la valutazione di impatto sulla protezione dei dati, il titolare del trattamento o il responsabile del trattamento dovrebbero consultarsi con il RPD, fra l'altro, sulle seguenti tematiche:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi ai requisiti in materia di protezione dei dati.

Per quanto riguarda il registro dei trattamenti, la sua tenuta è un obbligo che ricade sul titolare del trattamento o sul responsabile del trattamento, e non sul RPD. Cionondimeno, niente vieta al titolare del trattamento o al responsabile del trattamento di affidare al RPD il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso. Tale

registro va considerato uno degli strumenti che consentono al RPD di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare del trattamento o del responsabile del trattamento.

Fonte: articolo 39, paragrafo 1, lettera c) e articolo 30, RGPD

Fatto a Bruxelles, il 13 dicembre 2016

Per il Gruppo di lavoro,
La presidente
Isabelle FALQUE-PIERROTIN

Versione emendata e adottata in data 5 aprile 2017

Per il Gruppo di lavoro
La presidente
Isabelle FALQUE-PIERROTIN

NOTE

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119, 4.5.2016). Il RGPD è rilevante ai fini del SEE e sarà applicabile una volta incorporato nell'Accordo relativo al SEE.

[2] La nomina di un RPD è obbligatoria anche con riguardo alle autorità competenti di cui all'articolo 32 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119, 4.5.2016), alla luce della normativa nazionale di recepimento. Le presenti linee guida guardano con particolare attenzione alla figura del RPD come prevista dal RGPD, ma le indicazioni in esse formulate valgono anche per i RPD previsti dalla direttiva 2016/680 con riferimento alle disposizioni di carattere analogo contenute nei due strumenti.

[3] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (GU L 281, 23.11.95).

[4] Si veda http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf.

[5] Si osservi che, in base all'articolo 37, paragrafo 4, il diritto dell'Unione o dello Stato membro può prevedere casi ulteriori di nomina obbligatoria di un RPD.

[6] Con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali. V. articolo 32 della direttiva (UE) 2016/680.

[7] Ai sensi dell'articolo 9, si tratta dei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni filosofiche o religiose, o l'appartenenza sindacale, oltre al trattamento di dati genetici, dati biometrici al fine dell'identificazione univoca di una persona fisica, e di dati relativi alla salute, alla vita sessuale o all'orientamento sessuale di una persona fisica.

[8] Nel testo in lingua inglese dell'articolo 37, paragrafo 1, lettera c) compare la congiunzione "and" (e); si veda il paragrafo 2.1.5 infra per maggiori chiarimenti sull'utilizzo della congiunzione "o" anziché "e" nello specifico contesto.

[9] Articolo 10.

[10] Si veda l'articolo 24, paragrafo 1.

[11] Queste considerazioni valgono anche per i chief privacy officers (CPO) o altri professionisti in materia di privacy già operanti presso alcune aziende, che non sempre e non necessariamente si conformano ai requisiti fissati nel regolamento per quanto riguarda, per esempio, le risorse disponibili o le salvaguardie della loro indipendenza e che, in tal caso, non possono essere considerati e denominati "RPD".

[12] Si vedano, per esempio, le definizioni di "ente pubblico" e "organismo di diritto pubblico" contenute nell'articolo 2, paragrafi 1 e 2, della direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al

riutilizzo dell'informazione del settore pubblico.

[13] Articolo 6, paragrafo 1, lettera e).

[14] Il considerando in questione vi ricomprende, in particolare, "trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato". D'altro canto, lo stesso considerando prevede in modo specifico che "il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato". Si deve tener conto del fatto che il considerando offre alcune esemplificazioni ai due estremi della scala (trattamento svolto dal singolo medico / trattamento di dati relativi a un'intera nazione o a livello europeo) e che fra tali estremi si colloca un'ampia zona grigia. Inoltre, va sottolineato che il considerando citato si riferisce alle valutazioni di impatto sulla protezione dei dati; ciò significa che non tutti gli elementi citati sono necessariamente pertinenti alla nomina di un RPD negli stessi identici termini.

[15] "Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali."

[16] Si osservi che il considerando 24 riguarda l'applicazione extraterritoriale del RGPD; inoltre, vi è una differenza fra l'espressione "monitoraggio del loro comportamento" (articolo 3, paragrafo 2, lettera b)) e "monitoraggio regolare e sistematico degli interessati" (articolo 37, paragrafo 1, lettera b)), per cui le due espressioni potrebbero ben riferirsi a concetti distinti.

[17] Ai sensi della definizione contenuta all'articolo 4, punto 7, il titolare del trattamento è la persona o l'organismo che determina le finalità e i mezzi del trattamento.

[18] Ai sensi della definizione contenuta all'articolo 4, punto 8, il responsabile del trattamento è la persona o l'organismo che tratta dati personali per conto del titolare del trattamento.

[19] V. articolo 38, paragrafo 4: "Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento."

[20] V. articolo 39, paragrafo 1, lettera e): "fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione."

[21] Articolo 39, paragrafo 1, lettera a).

[22] V. anche paragrafo 2.6 infra.

[23] V. articolo 12, paragrafo 1: "Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori."

[24] V. articolo 39, paragrafo 1, lettera d: "cooperare con l'autorità di controllo."

[25] V. articolo 3 del RGPD per quanto concerne l'ambito territoriale di applicazione.

[26] Capo II.

[27] Capo III.

[28] Articolo 25.

[29] Articolo 30.

[30] Articolo 32.

[31] Articoli 33 e 34.

[32] Si osservi che l'articolo 33, paragrafo 3, lettera b), ove sono indicate le informazioni da fornire all'autorità di controllo e agli interessati in caso di violazione dei dati personali, prevede, a differenza dell'articolo 37, paragrafo 7, che tali informazioni comprendano anche il nominativo (e non solo le informazioni di contatto) del RPD.

[33] Articolo 35, paragrafo 2.

[34] Articolo 5, paragrafo 2.

[35] I compiti del RPD sono elencati all'articolo 39, paragrafo 1, ove si specifica che il RPD deve svolgere "almeno" i compiti in questione. Ne deriva che niente vieta al titolare di assegnare al RPD compiti ulteriori rispetto a quelli espressamente menzionati all'articolo 39, paragrafo 1, ovvero di specificare ulteriormente i suddetti compiti.

[36] L'articolo 24, paragrafo 1, prevede che "Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario".

[37] Si veda l'articolo 24, paragrafo 1, lettera d), del regolamento (CE) 45/2001.

Faq sul Responsabile della Protezione dei dati (RPD) in ambito privato (*) (in aggiunta a quelle adottate dal Gruppo Art. 29 in allegato alle Linee guida sul RPD)

1. Chi è il responsabile della protezione dei dati personali (RPD) e quali sono i suoi compiti?

Il responsabile della protezione dei dati personali (anche conosciuto con la dizione in lingua inglese data protection officer – DPO) è una figura prevista dall'art. 37 del Regolamento (UE) 2016/679. Si tratta di un soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Coopera con l'Autorità (e proprio per questo, il suo nominativo va comunicato al Garante; v. faq 6) e costituisce il

(*) *NDR. Questo documento è stato redatto dal Garante per la protezione dei dati personali e non adottato in ambito EDPB.*

punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (artt. 38 e 39 del Regolamento).

2. Quali requisiti deve possedere il responsabile della protezione dei dati personali?

Il responsabile della protezione dei dati personali, al quale non sono richieste specifiche attestazioni formali o l'iscrizione in appositi albi, deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento.
Deve poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Deve inoltre agire in piena indipendenza (considerando 97 del Regolamento UE 2016/679) e autonomia, senza ricevere istruzioni e riferendo direttamente ai vertici.
Il responsabile della protezione dei dati personali deve poter disporre, infine, di risorse (personale, locali, attrezzature, ecc.) necessarie per l'espletamento dei propri compiti.

3. Chi sono i soggetti privati obbligati alla sua designazione?

Sono tenuti alla designazione del responsabile della protezione dei dati personali il titolare e il responsabile del trattamento che rientrino nei casi previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679. Si tratta di soggetti le cui principali attività (in primis, le attività c.d. di "core business") consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali o di dati relative a condanne penali e a reati (per quanto attiene alle nozioni di "monitoraggio regolare e sistematico" e di "larga scala", v. le "Linee guida sui responsabili della protezione dei dati" del 5 aprile 2017, WP 243). Il diritto dell'Unione o degli Stati membri può prevedere ulteriori casi di designazione obbligatoria del responsabile della protezione dei dati (art. 37, par. 4).
Ricorrendo i suddetti presupposti, sono tenuti alla nomina, a titolo esemplificativo e non esaustivo: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; caf e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.

4. Chi sono i soggetti per i quali non è obbligatoria la designazione del responsabile della protezione dei dati personali?

Nei casi diversi da quelli previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679, la designazione del responsabile del trattamento non è obbligatoria (ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti: v. anche considerando 97 del Regolamento, in relazione alla definizione di attività "accessoria").
In ogni caso, resta comunque raccomandata, anche alla luce del principio di "accountability" che permea il Regolamento, la designazione di tale figura (v., in proposito, le menzionate linee guida), i cui criteri di nomina, in tale evenienza, rimangono gli stessi sopra indicati.

5. È possibile nominare un unico responsabile della protezione dei dati personali nell'ambito di un gruppo imprenditoriale?

Il Regolamento (UE) 2016/679 prevede che un gruppo imprenditoriale (v. definizione di cui all'art. 4, n. 19) possa designare un unico responsabile della protezione dei dati personali, purché tale responsabile sia facilmente raggiungibile da ciascuno stabilimento (sul concetto di "raggiungibilità", v. punto 2.3 delle linee guida in precedenza menzionate). Inoltre, dovrà essere in grado di comunicare in modo efficace con gli interessati e di collaborare con le autorità di controllo.

6. Il responsabile della protezione dei dati personali deve essere un soggetto interno o può essere anche un soggetto esterno? Quali sono le modalità per la sua designazione?

Il ruolo di responsabile della protezione dei dati personali può essere ricoperto da un dipendente del titolare o del responsabile (non in conflitto di interessi) che conosca la realtà operativa in cui avvengono i trattamenti; l'incarico può essere anche affidato a soggetti esterni, a condizione che garantiscano l'effettivo assolvimento dei compiti che il Regolamento (UE) 2016/679 assegna a tale figura. Il responsabile della protezione dei dati scelto all'interno andrà nominato mediante specifico atto di designazione, mentre quello scelto all'esterno, che dovrà avere le medesime prerogative e tutele di quello interno, dovrà operare in base a un contratto di servizi. Tali atti, da redigere in forma scritta, dovranno indicare espressamente i compiti attribuiti, le risorse assegnate per il loro svolgimento, nonché ogni altra utile informazione in rapporto al contesto di riferimento.
Nell'esecuzione dei propri compiti, il responsabile della protezione dei dati personali (interno o esterno) dovrà ricevere supporto adeguato in termini di risorse finanziarie, infrastrutturali e, ove opportuno, di personale. Il titolare o il responsabile del trattamento che abbia designato un responsabile per la protezione dei dati personali resta comunque pienamente responsabile dell'osser-

vanza della normativa in materia di protezione dei dati e deve essere in grado di dimostrarla (art. 5, par. 2, del Regolamento; v. anche i punti 3.2 e 3.3. delle linee guida sopra richiamate).
I dati di contatto del responsabile designato dovranno essere infine pubblicati dal titolare o responsabile del trattamento. Non è necessario - anche se potrebbe rappresentare una buona prassi - pubblicare anche il nominativo del responsabile della protezione dei dati: spetta al titolare o al responsabile e allo stesso responsabile della protezione dei dati, valutare se, in base alle specifiche circostanze, possa trattarsi di un'informazione utile o necessaria. Il nominativo del responsabile della protezione dei dati e i relativi dati di contatto vanno invece comunicati all'Autorità di controllo.

7. Il ruolo di responsabile della protezione dei dati personali è compatibile con altri incarichi?

Si, a condizione che non sia in conflitto di interessi. In tale prospettiva, appare preferibile evitare di assegnare il ruolo di responsabile della protezione dei dati personali a soggetti con incarichi di alta direzione (amministratore delegato; membro del consiglio di amministrazione; direttore generale; ecc.), ovvero nell'ambito di strutture aventi potere decisionale in ordine alle finalità e alle modalità del trattamento (direzione risorse umane, direzione marketing, direzione finanziaria, responsabile IT ecc.). Da valutare, in assenza di conflitti di interesse e in base al contesto di riferimento, l'eventuale assegnazione di tale incarico ai responsabili delle funzioni di staff (ad esempio, il responsabile della funzione legale).

8. Il responsabile della protezione dei dati personali è una persona fisica o può essere anche un soggetto diverso?

Il Regolamento (UE) 2016/679 prevede espressamente che il responsabile della protezione dei dati personali possa essere un "dipendente" del titolare o del responsabile del trattamento (art. 37, par. 6, del Regolamento); ovviamente, nelle realtà organizzative di medie e grandi dimensioni, il responsabile della protezione dei dati personali, da individuarsi comunque in una persona fisica, potrà essere supportato anche da un apposito ufficio dotato delle competenze necessarie ai fini dell'assolvimento dei propri compiti.
Qualora il responsabile della protezione dei dati personali sia individuato in un soggetto esterno, quest'ultimo potrà essere anche una persona giuridica (v. il punto 2.4 delle suddette Linee guida).
Si raccomanda, in ogni caso, di procedere a una chiara ripartizione di competenze, individuando una sola persona fisica atta a fungere da punto di contatto con gli interessati e l'Autorità di controllo.

Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico (*) (in aggiunta a quelle adottate dal Gruppo Art. 29 in allegato alle Linee guida sul RPD)

1. Quali sono i soggetti tenuti alla designazione del RPD, ai sensi dell'art. 37, par. 1, lett. a), del RGPD?

L'art. 37, par. 1, lett. a), del RGPD prevede che i titolari e i responsabili del trattamento designino un RPD «quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali».

Il RGPD non fornisce la definizione di "autorità pubblica" o "organismo pubblico" e, come chiarito anche nelle Linee guida adottate in materia dal Gruppo Art. 29 (di seguito Linee guida), ne rimette l'individuazione al diritto nazionale applicabile[1].

Allo stato, in ambito pubblico, devono ritenersi tenuti alla designazione di un RPD i soggetti che ricadevano nell'ambito di applicazione degli artt. 18-22 del Codice, che stabilivano le regole generali per i trattamenti effettuati dai soggetti pubblici (ad esempio, le amministrazioni dello Stato, anche con ordinamento autonomo, gli enti pubblici non economici nazionali, regionali e locali, le Regioni e gli enti

(*) *NDR. Questo documento è stato redatto dal Garante per la protezione dei dati personali e non adottato in ambito EDPB.*

locali, le università, le Camere di commercio, industria, artigianato e agricoltura, le aziende del Servizio sanitario nazionale, le autorità indipendenti ecc.).

Occorre, comunque, considerare che, nel caso in cui soggetti privati esercitino funzioni pubbliche (in qualità, ad esempio, di concessionari di servizi pubblici), può risultare comunque fortemente raccomandato, ancorché non obbligatorio, procedere alla designazione di un RPD. In ogni caso, qualora si proceda alla designazione di un RPD su base volontaria, si applicano gli identici requisiti - in termini di criteri per la designazione, posizione e compiti - che valgono per i RPD designati in via obbligatoria[2].

2. Nel caso in cui il RPD sia un dipendente dell'autorità pubblica o dell'organismo pubblico, quale qualifica deve avere?

Il RGPD non fornisce specifiche indicazioni al riguardo. È opportuno, in primo luogo, valutare se il complesso dei compiti assegnati al RPD - aventi rilevanza interna (consulenza, pareri, sorveglianza sul rispetto delle disposizioni) ed esterna (cooperazione con l'autorità di controllo e contatto con gli interessati in relazione all'esercizio dei propri diritti) - siano (o meno) compatibili con le mansioni ordinariamente affidate ai dipendenti con qualifica non dirigenziale.

In merito, l'art. 38, par. 3, del RGPD fissa alcune garanzie essenziali per consentire ai RPD di operare con un grado sufficiente di autonomia all'interno dell'organizzazione. In particolare, occorre assicurare che il RPD "non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti". Il considerando 97 aggiunge che i RPD "dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente". Ciò significa, come chiarito nelle Linee guida, che «il RPD, nell'esecuzione dei compiti attribuitigli ai sensi dell'articolo 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico – quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo. Né deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati».

Inoltre, sempre ai sensi dell'art. 38, par. 3, del RGPD, il RPD «riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento». Tale rapporto diretto garantisce, in particolare, che il vertice amministrativo venga a conoscenza delle indicazioni e delle raccomandazioni fornite dal RPD nell'esercizio delle funzioni di informazione e consulenza a favore del titolare o del responsabile.

Alla luce delle considerazioni di cui sopra, nel caso in cui si opti per un RPD interno, sarebbe quindi in linea di massima preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, la designazione sia conferita a un dirigente ovvero a un funzionario di alta professionalità, che possa svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione.

3. Quali certificazioni risultano idonee a legittimare il RPD nell'esercizio delle sue funzioni, ai sensi degli artt. 42 e 43 del RGPD?

Come accade nei settori delle cosiddette "professioni non regolamentate", si sono diffusi schemi proprietari di certificazione volontaria delle competenze professionali effettuate da appositi enti certificatori. Tali certificazioni (che non rientrano tra quelle disciplinate dall'art. 42 del RGPD) sono rilasciate anche all'esito della partecipazione ad attività formative e al controllo dell'apprendimento.

Esse, pur rappresentando, al pari di altri titoli, un valido strumento ai fini della verifica del possesso di un livello minimo di conoscenza della disciplina, tuttavia non equivalgono, di per sé, a una "abilitazione" allo svolgimento del ruolo del RPD né, allo stato, sono idonee a sostituire il giudizio rimesso alle PP.AA. nella valutazione dei requisiti necessari al RPD per svolgere i compiti previsti dall'art. 39 del RGPD[3].

4. Con quale atto formale deve essere designato il RPD?

Il RGPD prevede all'art. 37, par. 1, che il titolare e il responsabile del trattamento designino il RPD; da ciò deriva, quindi, che l'atto di designazione è parte costitutiva dell'adempimento.

Nel caso in cui la scelta del RPD ricada su una professionalità interna all'ente, occorre formalizzare un apposito atto di designazione a "Responsabile per la protezione dei dati". In caso, invece, di ricorso a soggetti esterni all'ente, la designazione costituirà parte integrante dell'apposito contratto di servizi redatto in base a quanto previsto dall'art. 37 del RGPD[4] (per agevolare gli enti, in allegato alle Faq, è riportato uno schema di atto di designazione).

Indipendentemente dalla natura e dalla forma dell'atto utilizzato, è necessario che nello stesso sia individuato in maniera inequivocabile il soggetto che opererà come RPD, riportandone espressamente le generalità[5], i compiti (eventualmente anche ulteriori a quelli previsti dall'art. 39 del RGPD[6]) e le funzioni che questi sarà chiamato a svolgere in ausilio al titolare/responsabile del trattamento, in conformità a quanto previsto dal quadro normativo di riferimento.

L'eventuale assegnazione di compiti aggiuntivi, rispetto a quelli originariamente previsti nell'atto di designazione, dovrà comportare la modifica e/o l'integrazione dello stesso o delle clausole contrattuali.

Nell'atto di designazione o nel contratto di servizi devono risultare succintamente indicate anche le motivazioni che hanno indotto l'ente a individuare, nella persona fisica selezionata, il proprio RPD, al fine di consentire la verifica del rispetto dei requisiti previsti dall'art. 37, par. 5 del RGPD, anche mediante rinvio agli esiti delle procedure di selezione interna o esterna effettuata. La specificazione dei criteri utilizzati nella valutazione compiuta dall'ente nella

scelta di tale figura, oltre a essere indice di trasparenza e di buon amministrazione, costituisce anche elemento di valutazione del rispetto del principio di «responsabilizzazione».

Una volta individuato, il titolare o il responsabile del trattamento è tenuto a indicare, nell'informativa fornita agli interessati, i dati di contatto del RPD pubblicando gli stessi anche sui siti web e a comunicarli al Garante (art. 37, par. 7). Per quanto attiene al sito web, può risultare opportuno inserire i riferimenti del RPD nella sezione "amministrazione trasparente", oltre che nella sezione "privacy" eventualmente già presente.

Come chiarito nelle Linee guida, in base all'art. 37, par. 7, non è necessario -anche se potrebbe costituire una buona prassi, in ambito pubblico- pubblicare anche il nominativo del RPD, mentre occorre che sia comunicato al Garante per agevolare i contatti con l'Autorità. Resta invece fermo l'obbligo di comunicare il nominativo agli interessati in caso di violazione dei dati personali (art. 33, par. 3, lett. b)[7].

5. La designazione di un RPD interno all'autorità pubblica o all'organismo pubblico richiede necessariamente anche la costituzione di un apposito ufficio?

Il RGPD prevede, all'art. 38, par. 2, che «il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica».

Ne discende che, in relazione alla complessità (amministrativa e tecnologica) dei trattamenti e dell'organizzazione, occorrerà valutare attentamente se una sola persona possa essere sufficiente a svolgere il complesso dei compiti affidati al RPD. Come riportato anche nelle Linee guida, «in linea di principio, quanto più aumentano complessità e/o sensibilità dei trattamenti, tanto maggiori devono essere le risorse messe a disposizione del RPD. La funzione "protezione dati" deve poter operare con efficienza e contare su risorse sufficienti in proporzione al trattamento svolto»[8].

All'esito di questa analisi si potrà valutare quindi l'opportunità/necessità di istituire un apposito ufficio al quale destinare le risorse necessarie allo svolgimento dei compiti stabiliti. Ad ogni modo, ove sia costituito un apposito ufficio, è comunque necessario che venga sempre individuata la persona fisica che riveste il ruolo di RPD (mediante l'atto di designazione di cui sopra)[9].

6. È ammissibile che uno stesso titolare/responsabile del trattamento abbia più di un RPD?

Alcune organizzazioni complesse hanno richiesto all'Autorità di valutare la possibilità di designare più RPD.

Al riguardo, si rileva che l'unicità della figura del RPD è una condizione necessaria per evitare il rischio di sovrapposizioni o incertezze sulle responsabilità, sia con riferimento all'ambito interno all'ente, sia con riferimento a quello esterno, e pertanto occorre che questa sia sempre assicurata.

Nulla osta, invece, all'individuazione di più figure di supporto, con riferimento a settori o ambiti territoriali diversi, anche dislocate presso diverse articolazioni organizzative dell'amministrazione, che facciano però riferimento a un unico soggetto responsabile, sia che la scelta ricada su un RPD interno, sia che questa ricada su un RPD esterno.

Infatti, in relazione alla particolare eterogeneità dei trattamenti di dati personali effettuati (in rapporto, ad esempio, all'effettuazione di trattamenti soggetti a basi giuridiche diverse in ambito di prevenzione, indagine, accertamento e perseguimento di reati) ovvero della complessità della struttura organizzativa dell'ente (talvolta molto ramificata a livello territoriale) può risultare opportuno individuare specifici "referenti" del RPD che potrebbero svolgere un ruolo di supporto e raccordo, sulla base di precise istruzioni del RPD, anche, se del caso, operando quali componenti del suo gruppo di lavoro[10].

7. Quali sono gli ulteriori compiti e funzioni che possono essere assegnati a un RPD?

Il RGPD consente l'assegnazione al RPD di ulteriori compiti e funzioni, a condizione che non diano adito a un conflitto di interessi (art. 38, par. 6e che consentano al RPD di avere a disposizione il tempo sufficiente per l'espletamento dei compiti previsti dal RGPD (art. 38, par. 2).

A seconda della natura dei trattamenti e delle attività e dimensioni della struttura del titolare o del responsabile, le eventuali ulteriori incombenze attribuite al RPD non dovrebbero pertanto sottrarre allo stesso il tempo necessario per adempiere alle relative responsabilità.

In linea di principio, è quindi ragionevole che negli enti pubblici di grandi dimensioni, con trattamenti di dati personali di particolare complessità e sensibilità, non vengano assegnate al RPD ulteriori responsabilità (si pensi, ad esempio, alle amministrazioni centrali, alle agenzie, agli istituti previdenziali, nonché alle regioni e alle asl). In tale quadro, ad esempio, avuto riguardo, caso per caso, alla specifica struttura organizzativa, alla dimensione e alle attività del singolo titolare o responsabile, l'attribuzione delle funzioni di RPD al responsabile per la prevenzione della corruzione e per la trasparenza, considerata la molteplicità degli adempimenti che incombono su tale figura, potrebbe rischiare di creare un cumulo di impegni tali da incidere negativamente sull'effettività dello svolgimento dei compiti che il RGPD attribuisce al RPD.

Rispetto all'assenza di conflitto di interessi, occorre inoltre valutare se, come indicato nelle Linee guida, le eventuali ulteriori funzioni assegnate non comportino la definizione di finalità e modalità del trattamento dei dati. Ciò signifi-

ca che, a grandi linee, in ambito pubblico, oltre ai ruoli manageriali di vertice, possono sussistere situazioni di conflitto di interesse rispetto a figure apicali dell'amministrazione investite di capacità decisionali in ordine alle finalità e ai mezzi del trattamento di dati personali posto in essere dall'ente pubblico, ivi compreso, ad esempio, il responsabile dei Sistemi informativi (chiamato ad individuare le misure di sicurezza necessarie), ovvero quello dell'Ufficio di statistica (deputato a definire le caratteristiche e le metodologie del trattamento dei dati personali utilizzati a fini statistici).

Riguardo agli ulteriori compiti e funzioni in capo al RPD, particolare attenzione andrebbe infine prestata nei casi di unico RPD tra molteplici autorità pubbliche e organismi pubblici, nonché nei casi di RPD esterno, in quanto questi potrebbe svolgere ulteriori compiti che comportano situazioni di conflitto di interesse oppure non essere in grado di adempiere in modo efficiente alle sue funzioni. In questi casi, nell'atto di designazione o nel contratto di servizio il RPD dovrà fornire opportune garanzie per favorire efficienza e correttezza e prevenire conflitti di interesse.

NOTE

[1] Cfr. al riguardo il par. 2.1.1., pag. 6, delle Linee guida sui responsabili della protezione dei dati (RPD) adottate dal Gruppo Art. 29 il 13 dicembre 2016 ed emendate il 5 aprile 2017 (WP243 rev. 01), disponibili sul sito istituzionale dell'Autorità.

[2] Anche in caso di assenza del requisito soggettivo previsto dall'art. 37, par. 1, lett. a), del RGPD, il titolare o il responsabile del trattamento sono comunque tenuti alla designazione del RPD, ai sensi di quanto previsto dall'art. 37, par. 1, lett. b) e c), nel caso in cui le attività principali consistano:

- in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala;
- nel trattamento su larga scala di categorie di dati personali di cui all'art. 9 del RGPD o dei dati relativi alle condanne penali e a reati di cui all'art. 10 del RGPD.

Con riferimento all'interpretazione delle espressioni «attività principali», «larga scala» e «monitoraggio regolare e sistematico» vedasi quanto riportato nelle Linee guida.

[3] Sul tema della certificazione inoltre si richiama l'attenzione sul comunicato congiunto, pubblicato sul sito dell'Autorità il 18 luglio 2017 (doc. web n. 6621723), con il quale il Garante e ACCREDIA (l'Ente unico nazionale di accreditamento designato dal Governo italiano) hanno ritenuto necessario sottolineare - al fine di indirizzare correttamente le attività svolte dai soggetti a vario titolo interessati in questo ambito - che «al momento le certificazioni di persone, nonché quelle emesse in materia di privacy o data protection eventualmente rilasciate in Italia, sebbene possano costituire una garanzia e atto di diligenza verso le parti interessate dell'adozione volontaria di un sistema di analisi e controllo dei principi e delle norme di riferimento, a legislazione vigente non possono definirsi "conformi agli artt. 42 e 43 del regolamento 2016/679", poiché devono ancora essere determinati i "requisiti aggiuntivi" ai fini dell'accreditamento degli organismi di certificazione e i criteri specifici di certificazione».

[4] Al riguardo, si ricorda che la funzione di RPD può essere esercitata anche in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna al titolare/responsabile del trattamento. In tal caso, come indicato nelle citate Linee guida, è indispensabile che ciascun soggetto appartenente alla persona giuridica operante quale RPD soddisfi tutti i requisiti richiesti dal RGPD. Cfr. sul punto le indicazioni del Gruppo Art. 29 riportate nel paragrafo 2.5., pag. 12, e nella domanda n. 7, pag. 24, delle Linee guida.

[5] Secondo quanto precisato nelle Linee guida, se la funzione di RPD è svolta da un fornitore esterno di servizi, i compiti stabiliti per il RPD potranno essere assolti efficacemente da un team operante sotto l'autorità di un contatto principale designato e "responsabile" per il singolo cliente. In particolare, «per favorire una corretta e trasparente organizzazione interna e prevenire conflitti di interesse a carico dei componenti il team RPD, si raccomanda di procedere a una chiara ripartizione dei compiti all'interno del team RPD e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente. Sarà utile, in via generale, inserire specifiche disposizioni in merito nel contratto di servizi» (cfr. par. 2.5., pag. 12).

[6] Cfr. la Faq n. 7 in relazione alla preliminare valutazione sulla compatibilità di ulteriori compiti e funzioni da assegnare al RPD.

[7] Cfr. al riguardo il paragrafo 2.6. delle Linee guida.

[8] Vedi sul punto Linee guida, paragrafo 3.2., pag. 15.

[9] Cfr., in proposito, la nota n. 4.

[10] In caso di RPD esterno, cfr. le note nn. 4 e 5.

Linee guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del regolamento (UE) 2016/679

Adottate il 23 gennaio 2019
Rettifica adottata il 9 aprile 2019[1]

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati),
visto l'accordo sullo Spazio economico europeo (SEE), in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del comitato misto SEE n. 154/2018 del 6 luglio 2018,

visto l'articolo 12 e l'articolo 22 del regolamento interno del 25 maggio 2018,

tenuto conto dei risultati della consultazione pubblica svoltasi tra il 30 maggio 2018 e il 12 luglio 2018 in conformità dell'articolo 70, paragrafo 4, del regolamento generale sulla protezione dei dati,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

Indice

1. INTRODUZIONE

2. Il regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679, nel prosieguo "il regolamento") istituisce un quadro di conformità aggiornato per la protezione dei dati in Europa, basato sul principio di responsabilizzazione e sulla tutela dei diritti fondamentali. Tale nuovo quadro è incentrato su una serie di misure atte ad agevolare la conformità alle disposizioni del regolamento generale sulla protezione dei dati, tra cui prescrizioni obbligatorie in circostanze specifiche (compresa la nomina di responsabili della protezione dei dati e lo svolgimento di valutazioni d'impatto sulla protezione dei dati) e misure volontarie come i codici di condotta e i meccanismi di certificazione.

3. Prima ancora che fosse adottato il regolamento generale sulla protezione dei dati il Gruppo di lavoro Articolo 29 aveva rilevato come la certificazione potesse rivestire un ruolo importante nel quadro di responsabilizzazione in materia di protezione dei dati[2]. Affinché la certificazione fornisca prove affidabili della conformità in termini di protezione dei dati è opportuno fissare norme chiare che introducano prescrizioni sull'erogazione della certificazione[3]. L'articolo 42 del regolamento generale sulla protezione dei dati fornisce la base giuridica per lo sviluppo di tali norme.

4. L'articolo 42, paragrafo 1, del regolamento generale sulla protezione dei dati stabilisce che:

   "[g]li Stati membri, le autorità di controllo, il Comitato [europeo per la protezione dei dati] e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese".

5. I meccanismi di certificazione[4] possono incrementare la trasparenza non solo per gli interessati, ma anche nel quadro delle relazioni tra imprese, per esempio tra titolare del trattamento e responsabile del trattamento. Il considerando 100 del regolamento generale sulla protezione dei dati rileva che l'istituzione di meccanismi di certificazione può migliorare la trasparenza e il rispetto del regolamento e consentire agli interessati di valutare il livello di protezione dei dati dei relativi prodotti e servizi[5].

6. Il regolamento generale sulla protezione dei dati non introduce alcun diritto od obbligo di certificazione per i titolari del trattamento e i responsabili del trattamento; come stabilito all'articolo 42, paragrafo 3, la certificazione è una procedura volontaria a sostegno della dimostrazione della conformità al regolamento. Gli Stati membri e le autorità di controllo sono invitati a incoraggiare l'istituzione di meccanismi di certificazione e de-

termineranno il coinvolgimento delle parti interessate nel processo e nel ciclo di vita della certificazione.

7. Le autorità di controllo sono inoltre tenute a considerare l'adesione a meccanismi di certificazione approvati come fattore aggravante o attenuante al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa (articolo 83, paragrafo 2, lettera j))[6].

1.1 AMBITO DI APPLICAZIONE DELLE LINEE GUIDA

8. Le presenti linee guida hanno un ambito di applicazione limitato e non costituiscono un manuale procedurale per la certificazione in conformità del regolamento generale sulla protezione dei dati. L'obiettivo primario delle presenti linee guida è identificare requisiti e criteri generali che possano applicarsi a tutti i tipi di meccanismi per le certificazioni rilasciate in conformità degli articoli 42 e 43 del regolamento generale sulla protezione dei dati. A tal fine le linee guida:

   - esplorano le motivazioni alla base della certificazione come strumento di responsabilizzazione,
   - illustrano i concetti chiave delle disposizioni in materia di certificazione di cui agli articoli 42 e 43,
   - illustrano ciò che può essere certificato a norma degli articoli 42 e 43 e lo scopo della certificazione,
   - favoriscono un esito della certificazione che sia significativo, inequivocabile, il più possibile riproducibile e comparabile a prescindere dal soggetto certificatore (comparabilità).

9. Il regolamento generale sulla protezione dei dati contempla una serie di modalità per l'attuazione degli articoli 42 e 43 da parte degli Stati membri e delle autorità di controllo. Le linee guida forniscono indicazioni sull'interpretazione e sull'attuazione delle disposizioni di cui agli articoli 42 e 43 e aiuteranno gli Stati membri, le autorità di controllo e gli organismi nazionali di accreditamento a istituire un approccio più coerente e armonizzato per l'applicazione dei meccanismi di certificazione in conformità del regolamento generale sulla protezione dei dati.

10. Le indicazioni contenute nelle linee guida saranno pertinenti per:

    - le autorità di controllo competenti e il Comitato europeo per la protezione dei dati, (il "Comitato") nella fase di approvazione dei criteri di certificazione in conformità dell'articolo 42, paragrafo 5, dell'articolo 58, paragrafo 3, lettera f), e dell'articolo 70, paragrafo 1, lettera o),
    - gli organismi di certificazione nella fase di definizione e revisione dei criteri di certificazione prima della presentazione all'autorità di controllo competente ai fini dell'approvazione a norma dell'articolo 42, paragrafo 5,

- il Comitato nella fase di approvazione di un sigillo europeo per la protezione dei dati a norma dell'articolo 42, paragrafo 5, e dell'articolo 70, paragrafo 1, lettera o),
- le autorità di controllo nella fase di definizione dei propri criteri di certificazione,
- la Commissione europea, a cui l'articolo 43, paragrafo 8, conferisce il potere di adottare atti delegati al fine di precisare i requisiti di cui tenere conto per i meccanismi di certificazione,
- il Comitato nella fase di presentazione alla Commissione di un parere in merito ai requisiti di certificazione in conformità dell'articolo 70, paragrafo 1, lettera q), e dell'articolo 43, paragrafo 8,
- gli organismi nazionali di accreditamento, che dovranno tenere conto dei criteri di certificazione nell'ottica dell'accreditamento degli organismi di certificazione in conformità della norma EN-ISO/IEC 17065/2012 e dei requisiti aggiuntivi in conformità dell'articolo 43, e
- i titolari del trattamento e i responsabili del trattamento durante la definizione della propria strategia di conformità al regolamento generale sulla protezione dei dati e la valutazione della certificazione come mezzo per dimostrare la conformità.

11. Il Comitato pubblicherà linee guida separate sull'identificazione dei criteri per l'approvazione dei meccanismi di certificazione come strumenti per il trasferimento verso paesi terzi o organizzazioni internazionali in conformità dell'articolo 42, paragrafo 2.

1.2 SCOPO DELLA CERTIFICAZIONE A NORMA DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

12. L'articolo 42, paragrafo 1, dispone l'istituzione di meccanismi di certificazione "allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento".

13. Il regolamento generale sulla protezione dei dati esemplifica il contesto in cui i meccanismi di certificazione approvati possono essere utilizzati come elementi per dimostrare il rispetto da parte del titolare del trattamento e del responsabile del trattamento dei loro obblighi riguardanti:

    - l'attuazione e la dimostrazione delle misure tecniche e organizzative adeguate di cui all'articolo 24, paragrafi 1 e 3, articolo 25 e articolo 32, paragrafi 1 e 3,
    - le garanzie sufficienti di cui all'articolo 28, paragrafi 1 (garanzie del responsabile del trattamento nei confronti del titolare del trattamento), 4 (garanzie del sub-responsabile del trattamento nei confronti del responsabile del trattamento) e 5.

14. La certificazione in sé non è una prova della conformità, ma rappresenta piuttosto un elemento che può essere utilizzato per dimostrare la conformità; è necessario pertanto che sia realizzata in modo trasparente. La dimostrazione della conformità necessita di una documentazione giustificativa, ossia di relazioni redatte appositamente che non si limitino a ribadire i criteri, ma illustrino le modalità con cui sono soddisfatti e, qualora inizialmente i criteri non fossero soddisfatti, illustrino le correzioni e le azioni correttive e la loro adeguatezza, esplicitando le ragioni del rilascio e del mantenimento della certificazione. Nella documentazione rientra anche il progetto della singola decisione per il rilascio, il rinnovo o il ritiro di un certificato, che dovrebbe riportare le ragioni, gli argomenti e le prove derivanti dall'applicazione dei criteri, nonché le conclusioni, le opinioni e le deduzioni derivanti dai fatti e dai presupposti rilevati durante la certificazione.

1.3 CONCETTI CHIAVE

15. La presente sezione esamina i concetti chiave di cui agli articoli 42 e 43. Tale analisi mira a fornire una comprensione dei termini di base e dell'ambito di applicazione della certificazione a norma del regolamento generale sulla protezione dei dati.

1.3.1 INTERPRETAZIONE DEL CONCETTO DI "CERTIFICAZIONE"

16. Il regolamento generale sulla protezione dei dati non fornisce una definizione di "certificazione". L'Organizzazione internazionale per la standardizzazione (ISO) fornisce una definizione universale di certificazione come "rilascio da parte di un organismo indipendente di un'assicurazione scritta (un certificato) del fatto che il prodotto, il servizio o il sistema in questione soddisfa requisiti specifici". La certificazione è nota anche come "valutazione della conformità di terza parte" mentre gli organismi di certificazione possono essere indicati anche con il termine "organismi di valutazione della conformità". Nella norma EN-ISO/IEC 17000:2004 "Valutazione della conformità — Vocabolario e principi generali" (a cui la ISO 17065 fa riferimento), la certificazione è definita come "attestazione di terza parte [...] relativa a prodotti, processi e servizi".

17. Per attestazione si intende "l'emissione di una dichiarazione, basata su una decisione successiva al riesame, da cui risulta che è stato dimostrato il rispetto di requisiti specifici" (sezione 5.2, ISO 17000:2004).

18. Nel contesto della certificazione a norma degli articoli 42 e 43 del regolamento generale sulla protezione dei dati si intende per certificazione l'attestazione di terza parte relativa a trattamenti effettuati dal titolare del trattamento e dal responsabile del trattamento.

1.3.2 MECCANISMI DI CERTIFICAZIONE, SIGILLI E MARCHI

19. Il regolamento generale sulla protezione dei dati non fornisce una definizione di "meccanismi di certificazione, sigilli o marchi" e utilizza i termini in senso collettivo. Un certificato è una dichiarazione di conformità. Un sigillo o un marchio può essere utilizzato per indicare che la procedura di certificazione è stata completata con esito positivo. Per sigillo o marchio si intende solitamente un logo o un simbolo la cui presenza (congiuntamente al certificato) indica che l'oggetto della certificazione è stato sottoposto a una valutazione indipendente nell'ambito di una procedura di certificazione ed è conforme a specifici requisiti fissati in documenti normativi come regolamenti, norme o specifiche tecniche. Nell'ambito della certificazione a norma del regolamento generale sulla protezione dei dati tali requisiti sono fissati nei requisiti aggiuntivi che integrano le regole per l'accreditamento degli organismi di certificazione di cui alla norma EN-ISO/IEC 17065/2012 e i criteri di certificazione approvati dall'autorità di controllo competente o dal Comitato. Un certificato, sigillo o marchio in conformità del regolamento generale sulla protezione dei dati può essere rilasciato solo a seguito di una valutazione indipendente degli elementi di prova ad opera di un organismo di certificazione accreditato o dell'autorità di controllo competente che attesti il soddisfacimento dei criteri di certificazione.

20. La tabella riporta un esempio generico di processo di certificazione.

Presentazione della domanda da parte del titolare del trattamento o del responsabile del trattamento	**Controllo formale da parte dell'organismo di certificazione**	**Valutazione preliminare**	**Valutazione dell'obiettivo di valutazione**	**Convalida dei risultati**	**Comunicazione all'autorità di controllo competente**	**Certificazione**	**Monitoraggio**	**Rinnovo della certificazione**
La descrizione dell'obiettivo di valutazione è inequivocabile e completa, nonché comprensiva delle interfacce?	La descrizione dell'obiettivo di valutazione può essere accettata?	Quali sono i criteri applicabili?	L'obiettivo di valutazione soddisfa i criteri?	L'obiettivo di valutazione rispecchia tutti i criteri pertinenti specificati?	Sono state fornite motivazioni per il rilascio o la revoca della certificazione?	Il certificato può essere rilasciato?	L'obiettivo di valutazione continua a soddisfare i criteri?	Il trattamento soddisfa ancora i criteri di certificazione?
È possibile accedere alle attività di trattamento dell'obiettivo di valutazione?	Tutti i documenti sono completi e aggiornati?	Quali sono i metodi di valutazione applicabili?	La documentazione dell'obiettivo di valutazione è corretta?	La valutazione è stata sufficientemente documentata?		Le relazioni sono pronte per la pubblicazione?	Il certificato/ sigillo/marchio di fiducia è utilizzato correttamente?	Gli ambiti di sviluppo sono stati adeguatamente presi in considerazione?
Articolo 42, paragrafo 6	Articolo 43, paragrafo 4	Articolo 43, paragrafo 4	Articolo 42, paragrafo 5, articolo 43, paragrafo 4	Articolo 43, paragrafo 4	Articolo 43, paragrafi 1 e 5	Articolo 43, paragrafo 1, articolo 42, paragrafo 7	Articolo 42, paragrafo 7	Articolo 42, paragrafo 7

2. IL RUOLO DELLE AUTORITÀ DI CONTROLLO

21. L'articolo 42, paragrafo 5, dispone che la certificazione sia rilasciata da un organismo di certificazione accreditato o da un'autorità di controllo competente. A norma del regolamento generale sulla protezione dei dati il rilascio delle certificazioni non è un compito obbligatorio delle autorità di controllo. Il regolamento prevede anzi una serie di modelli diversi. Un'autorità di controllo per esempio può optare per una o più delle seguenti soluzioni:

    - rilasciare essa stessa la certificazione, nel rispetto del proprio schema di certificazione,
    - rilasciare essa stessa la certificazione, nel rispetto del proprio schema di certificazione, ma delegare integralmente o parzialmente a terzi la procedura di valutazione,
    - predisporre un proprio schema di certificazione e affidare la procedura di certificazione per il rilascio della certificazione a organismi di certificazione, e
    - incoraggiare lo sviluppo di meccanismi di certificazione sul mercato.

22. Un'autorità di controllo dovrà inoltre considerare il proprio ruolo alla luce delle decisioni nazionali relative ai meccanismi di accreditamento, soprattutto laddove l'autorità di controllo ha essa stessa il potere di accreditare gli organismi di certificazione a norma dell'articolo 43, paragrafo 1, del regolamento generale sulla protezione dei dati. In questo modo ogni autorità di controllo deciderà quale approccio adottare per perseguire l'ampio obiettivo della certificazione conformemente al regolamento generale sulla protezione dei dati. Tale approccio sarà definito nell'ottica non solo dei compiti e dei poteri di cui gli articoli 57 e 58, ma anche del fatto che la certificazione dovrà essere considerata come un fattore di cui tenere conto nella determinazione delle sanzioni amministrative pecuniarie e più in generale come uno strumento per la dimostrazione della conformità.

2.1 L'AUTORITÀ DI CONTROLLO COME ORGANISMO DI CERTIFICAZIONE

23. Un'autorità di controllo, se decide di effettuare certificazioni, dovrà valutare attentamente il proprio ruolo in relazione ai compiti previsti dal regolamento generale sulla protezione dei dati. Essa dovrà esercitare le proprie funzioni in modo trasparente, prestando particolare attenzione alla separazione dei poteri di indagine e di esecuzione, al fine di evitare ogni potenziale conflitto di interessi.

24. Se agisce in qualità di organismo di certificazione, l'autorità di controllo dovrà garantire l'adeguata istituzione di un meccanismo di certificazione e adottare criteri di certificazione o svilupparne di propri. Ogni autorità di controllo che rilascia certificazioni ha inoltre il compito di sottoporle

a un riesame periodico (articolo 57, paragrafo 1, lettera o)) e il potere di revocarle se i requisiti per la certificazione non sono o non sono più soddisfatti (articolo 58, paragrafo 2, lettera h)). Per il soddisfacimento di tali requisiti è utile istituire una procedura di certificazione e requisiti procedurali, nonché, se non altrimenti disposto, ad esempio dalla legislazione nazionale, stipulare con le singole organizzazioni richiedenti un accordo legalmente valido per l'erogazione delle attività di certificazione. È auspicabile assicurarsi che tale accordo di certificazione imponga al richiedente di rispettare perlomeno i criteri di certificazione tra cui rientrano gli accorgimenti necessari per lo svolgimento della valutazione, il monitoraggio dell'adesione ai criteri e il riesame periodico, compreso l'accesso alle informazioni e/o ai locali, la documentazione e la pubblicazione delle relazioni e dei risultati, nonché lo svolgimento di indagini sui reclami. Si presume inoltre che l'autorità di controllo rispetti, oltre ai requisiti di cui all'articolo 43, paragrafo 2, anche i requisiti contenuti nelle linee guida relative all'accreditamento degli organismi di certificazione.

2.2 ULTERIORI COMPITI DELL'AUTORITÀ DI CONTROLLO IN MATERIA DI CERTIFICAZIONE

25. Negli Stati membri in cui operano organismi di certificazione l'autorità di controllo, indipendentemente dalle proprie attività, ha il potere e il compito di:

    - valutare i criteri dello schema di certificazione e predisporre un progetto di decisione (articolo 42, paragrafo 5),
    - comunicare al Comitato il progetto di decisione, qualora la decisione sia finalizzata ad approvare i criteri per la certificazione (articolo 64, paragrafo 1, lettera c) e articolo 64, paragrafo 7)), e tenere conto del parere del Comitato (articolo 64, paragrafo 1, lettera c) e articolo 70, paragrafo 1, lettera t)),
    - approvare i criteri per la certificazione (articolo 58, paragrafo 3, lettera f)) prima che possano essere effettuati accreditamenti o certificazioni (articolo 42, paragrafo 5, e articolo 43, paragrafo 2, lettera b)),
    - pubblicare i criteri di certificazione (articolo 43, paragrafo 6),
    - agire da autorità competente per gli schemi di certificazione a livello dell'UE, che possono risultare in un sigillo europeo per la protezione dei dati approvato dal Comitato (articolo 42, paragrafo 5, e articolo 70, paragrafo 1, lettera o)), e
    - ingiungere all'organismo di certificazione a) di non rilasciare la certificazione o b) di revocare la certificazione qualora i requisiti per la certificazione (procedure o criteri di certificazione) non siano o non siano più soddisfatti (articolo 58, paragrafo 2, lettera h)).

26. Il regolamento generale sulla protezione dei dati attribuisce all'autorità di controllo il compito di approvare i criteri di certificazione, ma non di svilupparli. Per approvare i criteri di certificazione a norma dell'articolo 42,

paragrafo 5, un'autorità di controllo deve avere una comprensione chiara di quanto aspettarsi, segnatamente in termini di ambito di applicazione e contenuti della dimostrazione di conformità al regolamento generale sulla protezione dei dati, nonché in merito al proprio compito di sorvegliare e assicurare l'applicazione del regolamento. L'allegato fornisce orientamenti mirati a garantire un approccio armonizzato nella valutazione dei criteri ai fini dell'approvazione.

27. A norma dell'articolo 43, paragrafo 1, gli organismi di certificazione sono tenuti a informare la rispettiva autorità di controllo competente prima di rilasciare o rinnovare le certificazioni, al fine di consentire alla stessa di esercitare i poteri correttivi di cui all'articolo 58, paragrafo 2, lettera h). L'articolo 43, paragrafo 5, impone inoltre agli organismi di certificazione di trasmettere all'autorità di controllo competente i motivi del rilascio o della revoca della certificazione richiesta. Sebbene il regolamento generale sulla protezione dei dati consenta alle autorità di controllo di determinare le modalità operative con cui ricevono, riconoscono, esaminano e gestiscono tali informazioni (tra cui per esempio soluzioni tecnologiche per consentire agli organismi di certificazione la trasmissione delle relazioni), è possibile istituire una procedura e i relativi criteri per il trattamento delle informazioni e delle relazioni fornite su ciascun progetto di certificazione andato a buon fine da parte dell'organismo di certificazione in conformità all'articolo 43, paragrafo 1. Sulla base di tali informazioni l'autorità di controllo può esercitare il proprio potere di ingiungere all'organismo di certificazione di revocare o non rilasciare una certificazione (articolo 58, paragrafo 2, lettera h)) e di sorvegliare e assicurare l'applicazione dei requisiti e dei criteri della certificazione a norma del regolamento generale sulla protezione dei dati (articolo 57, paragrafo 1, lettera a) e articolo 58, paragrafo 2, lettera h)). Ciò agevolerà un approccio armonizzato e la comparabilità delle certificazioni rilasciate da organismi di certificazione diversi, garantendo inoltre che le autorità di controllo siano a conoscenza delle informazioni relative allo stato della certificazione di un'organizzazione.

3. IL RUOLO DELL'ORGANISMO DI CERTIFICAZIONE

28. Il ruolo di un organismo di certificazione è di rilasciare, riesaminare, rinnovare e revocare le certificazioni (articolo 42, paragrafi 5 e 7) sulla base di un meccanismo di certificazione e di criteri approvati (articolo 43, paragrafo 1). L'organismo di certificazione o il proprietario dello schema di certificazione è tenuto pertanto a definire criteri di certificazione e a istituire procedure di certificazione, incluse procedure per il monitoraggio dell'adesione, lo svolgimento dei riesami, la gestione dei reclami e le revoche. I criteri di certificazione sono sottoposti a un riesame nell'ambito del processo di accreditamento, che tiene conto delle norme e delle procedure per il rilascio delle certificazioni, dei sigilli o dei marchi (articolo 43, paragrafo 2, lettera c)).

29. L'esistenza di un meccanismo di certificazione e di criteri di certificazione è indispensabile affinché l'organismo di certificazione possa essere accreditato a norma dell'articolo 43. L'attività dell'organismo di certificazione dipende in gran parte dall'ambito di applicazione e dal tipo di criteri di certificazione, che si ripercuotono sulle procedure di certificazione e viceversa. Determinati criteri per esempio potrebbero richiedere metodi di valutazione specifici, come sopralluoghi e revisioni di codici. Tali procedure sono obbligatorie ai fini dell'accreditamento e vengono illustrate più in dettaglio nelle linee guida relative all'accreditamento.

30. A norma del regolamento generale sulla protezione dei dati l'organismo di certificazione è tenuto a trasmettere alle autorità di controllo le informazioni, soprattutto relative alle singole certificazioni, necessarie per sorvegliare l'applicazione del meccanismo di certificazione (articolo 42, paragrafo 7, articolo 43, paragrafo 5, articolo 58, paragrafo 2, lettera h)).

4. L'APPROVAZIONE DEI CRITERI DI CERTIFICAZIONE

31. I criteri di certificazione sono parte integrante di qualsiasi meccanismo di certificazione. Il regolamento generale sulla protezione dei dati pertanto prevede che i criteri di certificazione di un meccanismo di certificazione debbano essere approvati dall'autorità di controllo competente (articolo 42, paragrafo 5, e articolo 43, paragrafo 2, lettera b)). Nel caso del sigillo europeo per la protezione dei dati i criteri di certificazione sono approvati dal Comitato (articolo 42, paragrafo 5, e articolo 70, paragrafo 1, lettera o)). Entrambe le modalità di approvazione dei criteri di certificazione sono illustrate di seguito.

32. Il Comitato riconosce le seguenti finalità per quanto riguarda l'approvazione dei criteri di certificazione:

    - rispecchiare adeguatamente i requisiti e i principi relativi alla protezione delle persone fisiche con riguardo al trattamento dei dati personali stabiliti dal regolamento (UE) n. 2016/679; e
    - contribuire alla coerente applicazione del regolamento generale sulla protezione dei dati.

33. L'approvazione è concessa se i criteri di certificazione rispecchiano perfettamente il requisito del regolamento generale sulla protezione dei dati per cui il meccanismo di certificazione consente ai titolari del trattamento e ai responsabili del trattamento di dimostrare la conformità al regolamento.

4.1 APPROVAZIONE DEI CRITERI DA PARTE DELL'AUTORITÀ DI CONTROLLO COMPETENTE

34. I criteri di certificazione devono essere approvati dall'autorità di control-

lo competente prima del processo di accreditamento di un organismo di certificazione o nel corso dello stesso. Anche gli schemi o gli insiemi di criteri aggiornati o aggiuntivi prodotti a cura dello stesso organismo di certificazione in conformità della norma ISO 17065 devono essere approvati prima di utilizzare i meccanismi di certificazione modificati (articolo 42, paragrafo 5 e articolo 43, paragrafo 2, lettera b)). Le autorità di controllo sono tenute a trattare tutte le richieste di approvazione dei criteri di certificazione in modo equo e non discriminatorio, in conformità di una procedura pubblica che specifichi le condizioni generali che dovranno essere soddisfatte e che descriva il processo di approvazione.

35. Un organismo di certificazione può rilasciare certificazioni solo in un determinato Stato membro in conformità dei criteri approvati dall'autorità di controllo di tale Stato membro. In altre parole i criteri di certificazione devono essere approvati dall'autorità di controllo competente del luogo in cui l'organismo di certificazione intende offrire la certificazione e ottiene l'accreditamento. Per i sistemi di certificazione a livello europeo si rimanda alla sezione seguente.

4.2 APPROVAZIONE DEI CRITERI RELATIVI AL SIGILLO EUROPEO PER LA PROTEZIONE DEI DATI DA PARTE DEL COMITATO

36. Un organismo di certificazione può inoltre rilasciare certificazioni conformemente ai criteri relativi al sigillo europeo per la protezione dei dati approvati dal Comitato. I criteri di certificazione approvati dal Comitato in conformità dell'articolo 63 possono dare luogo a un sigillo europeo per la protezione dei dati (articolo 42, paragrafo 5). Alla luce delle convenzioni attuali in materia di certificazione e accreditamento il Comitato riconosce che è auspicabile evitare una frammentazione del mercato delle certificazioni relative alla protezione dei dati. Il Comitato sottolinea come l'articolo 42, paragrafo 1, dispone che gli Stati membri, le autorità di controllo, il Comitato e la Commissione incoraggino l'istituzione di meccanismi di certificazione, in particolare a livello di Unione.

4.2.1 DOMANDA DI APPROVAZIONE

37. La domanda per l'approvazione dei criteri da parte del Comitato a norma dell'articolo 42, paragrafo 5, e dell'articolo 70, paragrafo 1, lettera o), deve essere presentata tramite un'autorità di controllo competente e dovrebbe esplicitare l'intenzione del proprietario dello schema, del candidato o dell'organismo di certificazione accreditato di predisporre i criteri nell'ambito di un meccanismo di certificazione destinato ai titolari del trattamento e ai responsabili del trattamento in tutti gli Stati membri. L'autorità di controllo competente, se ritiene che i criteri possono essere approvati dal Comitato, trasmette al Comitato un progetto.

38. La scelta del luogo in cui presentare la domanda per l'approvazione dei criteri si baserà sulla sede principale dell'organizzazione proprietaria dello schema di certificazione o dell'organismo di certificazione.
39. Se un organismo di certificazione presenta una domanda, esso starà di norma richiedendo l'accreditamento o sarà già accreditato dall'autorità di controllo competente o dall'organismo nazionale di accreditamento del proprio Stato membro. Il fatto che un organismo di certificazione sia già accreditato per un meccanismo di certificazione a norma del regolamento generale sulla protezione dei dati può contribuire a velocizzare il processo di approvazione.

4.2.2 CRITERI RELATIVI AL SIGILLO EUROPEO PER LA PROTEZIONE DEI DATI

40. Il Comitato coordinerà il processo di valutazione e approverà i criteri relativi al sigillo europeo per la protezione dei dati come previsto. Tale valutazione prenderà in considerazione aspetti quali l'ambito di applicazione dei criteri e la loro idoneità a fungere da certificazione comune. Qualora i criteri siano approvati dal Comitato, è previsto che sia l'autorità di controllo competente per la sede principale dell'organismo di certificazione all'interno dell'UE a gestire i reclami riguardanti il meccanismo stesso e a informare le altre autorità di controllo. Tale autorità di controllo inoltre ha il compito di adottare provvedimenti nei confronti dell'organismo di certificazione. Ove opportuno, l'autorità di controllo competente informerà le altre autorità di controllo e il Comitato.

41. Criteri di certificazione relativi a una certificazione comune sono soggetti a richieste provenienti da tutta l'UE e pertanto dovrebbero contemplare un meccanismo specifico atto a far fronte a tali richieste. I meccanismi di certificazione europei devono essere progettati per l'utilizzo in tutti gli Stati membri. In virtù dell'articolo 42, paragrafo 5, è necessario che il meccanismo del sigillo europeo per la protezione dei dati e i relativi criteri siano adattabili in modo da poter tenere conto, se del caso, delle regolamentazioni settoriali nazionali, per esempio in materia di trattamento dei dati nelle scuole, e che contemplino l'applicazione su tutto il territorio europeo.

42. Esempio: una scuola internazionale che offre servizi di istruzione a interessati nell'Unione europea ha la propria sede nello Stato membro "A". La scuola desidera certificare la propria procedura di iscrizione online tramite uno schema di certificazione a livello europeo per ottenere il sigillo europeo per la protezione dei dati. La scuola intende richiedere la certificazione delle proprie operazioni di trattamento a un organismo di certificazione avente sede in uno Stato membro "B" sulla base del sigillo europeo per la protezione dei dati. I criteri per il sigillo progettati e documentati nell'ambito del meccanismo pertinente devono poter tener conto delle regolamentazioni relative alle scuole applicabili nello Stato membro "A". I criteri inoltre dovrebbero prevedere che la procedura di iscrizione

online fornisca informazioni e tenga conto dei requisiti di protezione dei dati applicabili nello Stato membro, che potrebbero differire da quelli degli altri Stati membri, ad esempio in termini di dati personali da presentare ai fini della candidatura, come valutazioni o risultati dei test presso la scuola dell'infanzia, periodi di conservazione, raccolta o trattamento di dati finanziari o biometrici e ulteriori limitazioni del trattamento.

- Tra i criteri di alto livello per l'approvazione di un meccanismo relativo al sigillo europeo per la protezione dei dati figurano:

  - criteri approvati dal Comitato,
  - applicazione in tutti gli Stati membri, che tenga conto, se del caso, dei requisiti di legge e delle regolamentazioni settoriali nazionali,
  - criteri armonizzati adattabili in modo da rispecchiare i requisiti nazionali,
  - una descrizione del meccanismo di certificazione che specifichi:
  - gli accordi di certificazione, che devono prevedere requisiti paneuropei,
  - le procedure atte a garantire la diversificazione nazionale e a fornire soluzioni in tal senso, nonché ad assicurare che il sigillo agevoli la dimostrazione della conformità al regolamento generale sulla protezione dei dati, e
  - la lingua delle relazioni indirizzate a tutte le autorità di controllo interessate.

43. L'allegato contiene ulteriori indicazioni sui criteri relativi al sigillo europeo per la protezione dei dati.

4.2.3 RUOLO DELL'ACCREDITAMENTO

44. Come evidenziato al punto 4.2.1, una volta individuati criteri idonei a configurare una certificazione comune, approvati come tali dal Comitato a norma dell'articolo 42, paragrafo 5, è possibile accreditare organismi di certificazione per lo svolgimento delle certificazioni a livello europeo in conformità di tali criteri.

45. Gli schemi progettati per essere offerti solo in determinati Stati membri non possono candidarsi per ottenere il sigillo UE. L'accreditamento per l'ambito di applicazione del sigillo europeo per la protezione dei dati richiederà l'accreditamento nello Stato membro della sede principale dell'organismo di certificazione che intende utilizzare lo schema, ossia l'organismo responsabile del rilascio delle certificazioni e della gestione delle attività di certificazione delle proprie entità e affiliate in altri Stati membri. Laddove altri stabilimenti o uffici gestiscano ed effettuino certificazioni in autonomia, ciascuno di tali stabilimenti o uffici dovrà essere accreditato separatamente nello Stato membro in cui ha sede. In altre parole, se è solo la sede principale a rilasciare i certificati, l'accreditamento

è necessario esclusivamente nello Stato membro della sede principale. Se invece i certificati sono rilasciati anche da altri stabilimenti dell'organismo di certificazione, anche tali stabilimenti devono essere accreditati.

46. Di conseguenza, se un organismo di certificazione non è stato accreditato per lo svolgimento di attività di certificazione a norma del sigillo europeo per la protezione dei dati, i criteri approvati dal Comitato non possono essere utilizzati e il sigillo non può essere rilasciato.

5. SVILUPPO DI CRITERI DI CERTIFICAZIONE

47. Il regolamento generale sulla protezione dei dati ha definito il quadro di riferimento per lo sviluppo di criteri di certificazione. Sebbene gli articoli 42 e 43 stabiliscano le prescrizioni fondamentali relative alla procedura di certificazione nonché i criteri essenziali per tali procedure, il fondamento per la definizione dei criteri di certificazione dev'essere rinvenuto nei principi e nelle norme del regolamento generale sulla protezione dei dati e deve contribuire a garantire il rispetto di tali principi e norme.

48. Lo sviluppo di criteri di certificazione dovrebbe concentrarsi sulla verificabilità, la rilevanza e l'idoneità di tali criteri ai fini della dimostrazione della conformità al regolamento. I criteri di certificazione dovrebbero essere formulati in modo da essere chiari, comprensibili e applicabili nella pratica.

49. Nella definizione di criteri di certificazione si dovrebbe tenere conto tra l'altro dei seguenti aspetti di conformità a sostegno della valutazione dell'operazione di trattamento, se applicabili:

- la liceità del trattamento a norma dell'articolo 6,
- i principi del trattamento di dati personali a norma dell'articolo 5,
- i diritti degli interessati a norma degli articoli da 12 a 23,
- l'obbligo di notifica delle violazioni dei dati a norma dell'articolo 33,
- l'obbligo della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita a norma dell'articolo 25,
- se è stata effettuata o meno una valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35, paragrafo 7, lettera d), se pertinente, e
- le misure tecniche e organizzative messe in atto a norma dell'articolo 32.

50. La misura in cui i criteri rispecchiano tali aspetti può variare a seconda dell'ambito di applicazione della certificazione, alla cui definizione possono contribuire il tipo di trattamento o trattamenti e il settore oggetto della certificazione (per esempio il settore sanitario).

5.1 CHE COSA PUÒ ESSERE CERTIFICATO A NORMA DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI?

51. Il Comitato ritiene che il regolamento generale sulla protezione dei dati configuri un ambito esteso in termini di ciò che può essere certificato a norma del regolamento stesso, purché la certificazione sia mirata a dimostrare la conformità al regolamento di trattamenti effettuati da titolari e responsabili (articolo 42, paragrafo 1).

52. Nella valutazione di un trattamento devono essere presi in considerazione, se pertinenti, i tre elementi chiave seguenti:

    1. dati personali (ambito di applicazione materiale del regolamento generale sulla protezione dei dati);
    2. sistemi tecnici, ovvero le infrastrutture, ad esempio strumenti hardware e software, utilizzate per trattare i dati personali; e
    3. i processi e le procedure relative al trattamento o ai trattamenti.

53. Ciascun elemento utilizzato nei trattamenti deve essere sottoposto a valutazione sulla base dei criteri predefiniti. Almeno quattro diversi fattori significativi possono influire sul trattamento: 1) l'organizzazione e la struttura giuridica del titolare del trattamento o del responsabile del trattamento; 2) l'unità o divisione, l'ambiente e le persone coinvolte nel trattamento o nei trattamenti; 3) la descrizione tecnica degli elementi oggetto della valutazione; e infine 4) l'infrastruttura informatica a supporto del trattamento, compresi sistemi operativi, sistemi virtuali, banche dati, sistemi di autenticazione e autorizzazione, router e firewall, sistemi di archiviazione, infrastrutture di comunicazione o accesso a Internet e misure tecniche correlate.

54. Tutti e tre gli elementi chiave sono rilevanti ai fini della progettazione delle procedure e dei criteri di certificazione. La misura in cui sono presi in considerazione varia a seconda dell'oggetto della certificazione. In taluni casi ad esempio alcuni elementi possono non essere considerati, se non sono ritenuti pertinenti per l'oggetto della certificazione.

55. Il regolamento generale sulla protezione dei dati offre ulteriori orientamenti volti a specificare maggiormente che cosa può essere certificato a norma del regolamento stesso. In base all'articolo 42, paragrafo 7, le certificazioni a norma del regolamento generale sulla protezione dei dati sono rilasciate solo ai titolari del trattamento o ai responsabili del trattamento, il che esclude ad esempio la certificazione dei responsabili della protezione dei dati. L'articolo 43, paragrafo 1, lettera b), cita la norma ISO 17065, che disciplina l'accreditamento degli organismi di certificazione che valutano la conformità di prodotti, servizi e processi. Un trattamento o un insieme di trattamenti potrebbero dare luogo a un prodotto o a un servizio quali definiti dalla norma ISO 17065 e pertanto possono essere sottoposti alla certificazione. Il trattamento dei dati dei dipendenti ai fini del versamento dello stipendio

o della gestione delle ferie, per esempio, è un insieme di operazioni ai sensi del regolamento generale sulla protezione dei dati e può dare luogo a un prodotto, processo o servizio quale definito dall'ISO.

56. Sulla base di tali considerazioni il Comitato ritiene che l'ambito di applicazione della certificazione a norma del regolamento generale sulla protezione dei dati sia rivolto ai trattamenti e agli insiemi di trattamenti. Tra questi possono rientrare i processi di governance intesi come misure organizzative, quindi come parti integranti di un trattamento (ad esempio il processo di governance istituito per la gestione dei reclami nell'ambito del trattamento dei dati dei dipendenti ai fini del versamento dello stipendio).

57. Per valutare la conformità del trattamento ai criteri di certificazione è necessario indicare un caso d'uso. Per esempio, la conformità dell'utilizzo di un'infrastruttura tecnica nell'ambito di un trattamento dipende dalle categorie di dati per il cui trattamento tale infrastruttura è stata progettata. Le misure organizzative dipendono dalle tipologie e dal volume dei dati e dall'infrastruttura utilizzata per il trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, oltre che dei rischi per i diritti e le libertà degli interessati.

58. Occorre tenere presente inoltre che le applicazioni informatiche possono differire di gran lunga le une dalle altre anche quando sono destinate alle stesse finalità di trattamento. Tale aspetto deve essere pertanto tenuto in considerazione nel definire l'ambito di applicazione dei meccanismi di certificazione e i criteri di certificazione; in altre parole l'ambito di applicazione della certificazione e i rispettivi criteri non dovrebbero essere tanto ristretti da escludere applicazioni informatiche progettate diversamente.

5.2 DEFINIZIONE DELL'OGGETTO DELLA CERTIFICAZIONE

59. Occorre distinguere l'ambito di applicazione di un meccanismo di certificazione dall'oggetto della certificazione, anche detto oggetto della valutazione, ODV, identificato nel singolo progetto di certificazione in conformità di un meccanismo di certificazione. Un meccanismo di certificazione può definire il proprio ambito di applicazione in linea generale oppure in riferimento a una specifica tipologia o settore di trattamento, e in quest'ultimo caso potranno essere identificati in partenza gli oggetti della certificazione che rientrano nell'ambito di applicazione del meccanismo di certificazione (ad esempio, conservazione sicura e protezione dei dati personali contenuti nelle cassette di sicurezza digitali). In ogni caso una valutazione affidabile e significativa della conformità può avvenire solo previa descrizione precisa del singolo oggetto di un progetto di certificazione. Devono essere descritti chiaramente i trattamenti inclusi nell'oggetto della certificazione e quindi gli elementi chiave, ossia quali dati, processi e infrastrutture tecniche saranno sottoposti a valutazione e quali

no. In tale quadro dovranno sempre essere prese in considerazione e descritte le eventuali interfacce con altri processi. Ovviamente ciò che non è noto non può essere parte della valutazione e quindi non potrà essere certificato. In ogni caso il singolo oggetto della certificazione deve essere significativo rispetto al messaggio o allo slogan della certificazione, e non dovrebbe trarre in inganno l'utente, il cliente o il consumatore.

60. ***[Esempio 1]***
Una banca offre ai propri clienti un sito Internet per effettuare operazioni bancarie online. Tale servizio permette di effettuare bonifici, comprare azioni, avviare ordini permanenti e gestire il conto. La banca desidera certificare quanto segue in conformità di un meccanismo di certificazione in materia di protezione dei dati con un ambito di applicazione generale basato su criteri generici.

a) Log-in sicuro
Il log-in sicuro rappresenta un'operazione di trattamento comprensibile per l'utente finale e pertinente sotto il profilo della protezione dei dati in quanto riveste un ruolo importante nella garanzia della sicurezza dei dati personali in questione. Tale trattamento pertanto è necessario per garantire la sicurezza del login e perciò può rappresentare un oggetto di valutazione significativo, a condizione che il certificato indichi chiaramente che viene certificato solo il trattamento del log-in.

b) Front-end web
Pur essendo rilevante sotto il profilo della protezione dei dati, il front-end web non è comprensibile per l'utente finale e pertanto non può costituire un oggetto di valutazione significativo. Per l'utente inoltre non è chiaro quali dei servizi disponibili sul sito web, e quindi quali trattamenti, siano coperti dalla certificazione.

c) Servizi bancari online
Front-end e back-end web, se considerati congiuntamente, rappresentano trattamenti erogati nell'ambito dei servizi bancari online potenzialmente significativi per l'utente finale. In tale contesto entrambi devono essere inseriti nell'oggetto della valutazione. Al contrario i trattamenti non direttamente collegati alla fornitura di servizi bancari online, come ad esempio i trattamenti finalizzati alla prevenzione del riciclaggio di denaro, possono essere esclusi dall'ODV.

È possibile tuttavia che tra i servizi di operazioni bancarie online offerti dalla banca tramite il proprio sito web rientrino altri servizi che a loro volta richiedono propri trattamenti. Uno di questi servizi ulteriori in tale contesto potrebbe essere l'offerta di un prodotto assicurativo. Tale servizio aggiuntivo non è collegato direttamente con la finalità di fornire servizi bancari online e perciò può essere escluso dall'oggetto della valutazione. Sebbene tale servizio aggiuntivo (assicurazione) sia escluso dall'ODV, le interfacce per l'accesso a tale servizio integrate sul sito web rientrano nell'ODV stesso e, pertanto, devono essere descritte in modo da consentire una netta distinzione tra i servizi. Tale descrizione è necessaria per identificare e valutare possibili flussi di dati tra i due servizi.

61. ***[Esempio 2]***
Una banca offre ai propri clienti un servizio che consente loro di aggregare informazioni relative a conti diversi e a carte di credito emesse da più banche (aggregazione dei conti). La banca desidera certificare il proprio servizio in conformità del regolamento generale sulla protezione dei dati. L'autorità di controllo competente ha approvato criteri di certificazione specifici per questo tipo di attività. Nell'ambito di applicazione del meccanismo di certificazione rientrano solo i seguenti aspetti di conformità:

- *autenticazione dell'utente, e*
- *modalità accettabili per ottenere dalle altre banche/dagli altri servizi i dati che devono essere aggregati.*

Poiché l'ambito di applicazione di tale meccanismo di certificazione già di per sé definisce l'oggetto della valutazione, non è possibile restringerlo ulteriormente in maniera significativa all'interno dell'ambito di applicazione proposto e certificare solo caratteristiche specifiche o una singola attività di trattamento. In questo caso l'oggetto della valutazione coincide necessariamente con un ambito di applicazione specifico.

5.3 METODI DI VALUTAZIONE E METODOLOGIA DELLA VALUTAZIONE

62. Per una valutazione di conformità finalizzata a dimostrare la conformità dei trattamenti occorre identificare e definire i metodi per la valutazione e la metodologia della valutazione. È importante stabilire se le informazioni utilizzate per la valutazione sono raccolte esclusivamente attraverso documentazione (cosa che in sé non sarebbe sufficiente) o se sono raccolte attivamente in loco, e tramite accesso diretto o indiretto. La modalità di raccolta delle informazioni si ripercuote sulla rilevanza della certificazione e pertanto dovrebbe essere definita e descritta.

Le procedure per il rilascio e il riesame periodico delle certificazioni dovrebbero comprendere specifiche atte a identificare il livello di valutazione adeguato (in termini di profondità e granularità) per soddisfare i criteri di certificazione, nonché contemplare:

- informazioni e indicazioni specifiche sui metodi di valutazione applicati e sulle risultanze raccolte, per esempio nell'ambito di controlli in loco o a partire dalla documentazione,
- metodi di valutazione incentrati sui trattamenti (dati, sistemi, processi) e sulle finalità del trattamento,
- l'identificazione delle categorie di dati, delle esigenze di protezione e dell'eventuale coinvolgimento di responsabili del trattamento o di terzi,
- l'identificazione dei ruoli e l'esistenza di un meccanismo di controllo degli accessi che definisca ruoli e responsabilità.

63. La profondità della valutazione si ripercuote sulla rilevanza e sul valore della certificazione. Una riduzione della profondità della valutazione per

scopi pratici o per contenere i costi si tradurrà in una minore rilevanza della certificazione in materia di protezione dei dati. Le decisioni sulla granularità della valutazione d'altro canto potrebbero superare la capacità finanziaria del richiedente e spesso anche le capacità di valutatori e revisori. Ai fini della dimostrazione della conformità, potrebbe non essere sempre indispensabile raggiungere un livello molto dettagliato di analisi dei sistemi informatici utilizzati per mantenere la significatività.

5.4 DOCUMENTAZIONE DELLA VALUTAZIONE

64. La documentazione di certificazione dovrebbe essere accurata ed esauriente. Una lacuna nella documentazione si traduce nell'impossibilità di effettuare una valutazione corretta. La funzione essenziale della documentazione di certificazione è garantire la trasparenza del processo di valutazione nel quadro del meccanismo di certificazione. La documentazione fornisce risposte relative ai requisiti previsti per legge. I meccanismi di certificazione dovrebbero prevedere una metodologia di documentazione standardizzata. Successivamente la valutazione consentirà di confrontare la documentazione di certificazione con la situazione corrente in loco e con i criteri di certificazione.

65. Una documentazione esauriente di quanto è stato certificato e della metodologia utilizzata è funzionale a una maggiore trasparenza. A norma dell'articolo 43, paragrafo 2, lettera c), i meccanismi di certificazione dovrebbero prevedere procedure che consentano il riesame delle certificazioni. Una documentazione dettagliata potrebbe essere il mezzo di comunicazione più indicato per consentire all'autorità di controllo di valutare se e in quale misura tenere conto della certificazione nell'ambito di indagini formali. È pertanto opportuno che la documentazione prodotta nel corso della valutazione si concentri su tre aspetti fondamentali:

    - coerenza dei metodi di valutazione impiegati,
    - metodi di valutazione mirati a dimostrare la conformità dell'oggetto della certificazione ai criteri di certificazione e quindi al regolamento, e
    - convalida dei risultati della valutazione da parte di un organismo di certificazione indipendente e imparziale.

5.5 DOCUMENTAZIONE DEI RISULTATI

66. Il considerando 100 fornisce informazioni sugli obiettivi perseguiti con l'introduzione della certificazione.

    "Al fine di migliorare la trasparenza e il rispetto del presente regolamento dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi."

67. La documentazione e la comunicazione dei risultati rivestono un ruolo importante ai fini del miglioramento della trasparenza. Gli organismi di certificazione che utilizzano meccanismi di certificazione, sigilli o marchi rivolti agli interessati (in qualità di consumatori o clienti) dovrebbero fornire informazioni facilmente accessibili, comprensibili e significative riguardo al trattamento o ai trattamenti certificati. Tali informazioni pubbliche dovrebbero comprendere almeno:

- la descrizione dell'oggetto della valutazione,
- l'indicazione dei criteri approvati applicati all'oggetto della valutazione in questione,
- la metodologia di valutazione dei criteri (valutazione in loco, documentazione ecc.), e
- il periodo di validità del certificato, e
- dovrebbero consentire alle autorità di controllo e al pubblico la comparabilità dei risultati.

6. ORIENTAMENTI PER LA DEFINIZIONE DEI CRITERI DI CERTIFICAZIONE

68. I criteri di certificazione sono parte integrante di un meccanismo di certificazione. Nella procedura di certificazione rientrano requisiti riguardanti le modalità, gli autori, l'entità e la granularità della valutazione che sarà effettuata all'interno dei singoli progetti di certificazione relativi a uno specifico oggetto di valutazione. I criteri di certificazione stabiliscono i requisiti nominali a fronte dei quali è valutato il trattamento effettivo definito nell'oggetto di valutazione. Le presenti linee guida per la definizione dei criteri di certificazione forniscono indicazioni di massima per agevolare la valutazione dei criteri di certificazione ai fini dell'approvazione.

- Nell'ambito dell'approvazione o della definizione dei criteri di certificazione è opportuno tenere presenti le considerazioni generali illustrate di seguito. I criteri di certificazione dovrebbero:
- essere uniformi e verificabili,
- specificare in particolare i propri obiettivi e gli orientamenti attuativi per raggiungere tali obiettivi, in modo tale da poter essere sottoposti a controlli volti ad agevolare la valutazione dei trattamenti a norma del regolamento generale sulla protezione dei dati,
- essere pertinenti rispetto al pubblico a cui si rivolgono (relazioni tra imprese oppure relazioni tra imprese e clienti),
- tenere conto di eventuali altre norme (ad esempio norme ISO o norme a livello nazionale) e laddove opportuno essere interoperabili con le stesse,
- essere flessibili e scalabili in modo da applicarsi a organizzazioni di diverso tipo e dimensione, comprese le micro, piccole e medie imprese in conformità dell'articolo 42, paragrafo 1, nonché da rispecchiare l'approccio basato sul rischio di cui al considerando 77.

69. Una piccola società locale, ad esempio un rivenditore al dettaglio, di norma effettuerà trattamenti meno complessi di una grande multinazionale di vendita. Sebbene le prescrizioni relative alla liceità del trattamento siano le stesse, occorre tenere conto dell'ambito di applicazione del trattamento dei dati e della sua complessità; è necessario pertanto che i meccanismi di certificazione e i loro criteri siano scalabili sulla base dell'attività di trattamento in questione.

6.1 NORME ESISTENTI

70. Gli organismi di certificazione dovranno considerare in che modo gli specifici criteri tengono conto degli strumenti pertinenti già in essere, come ad esempio codici di condotta, norme tecniche o iniziative legislative e di regolamentazione a livello nazionale. Idealmente i criteri saranno interoperabili con le norme esistenti atte ad agevolare un titolare del trattamento o un responsabile del trattamento nell'ottemperanza ai propri obblighi previsti dal regolamento generale sulla protezione dei dati. Tuttavia, mentre le norme di settore spesso si concentrano sulla protezione e sulla sicurezza delle organizzazioni nei confronti di eventuali minacce, il regolamento generale sulla protezione dei dati è incentrato sulla protezione dei diritti fondamentali delle persone fisiche. Nella progettazione dei criteri o nell'approvazione dei criteri o dei meccanismi di certificazione sulla base delle norme di settore si dovrà tener conto di tale differenza di prospettiva.

6.2 DEFINIZIONE DEI CRITERI

71. I criteri di certificazione devono corrispondere alla dichiarazione di certificazione (messaggio o indicazione) di un dato meccanismo o schema di certificazione e soddisfare le aspettative create dalla stessa. La denominazione di un meccanismo di certificazione può già identificare l'ambito di applicazione e ripercuotersi sulla definizione dei criteri.

72. ***[Esempio 3]***
L'ambito di applicazione di un meccanismo denominato "MarchioPrivacySanità" dovrebbe essere ristretto al solo settore sanitario. Dato il nome del sigillo ci si aspetta infatti che siano stati esaminati i requisiti di protezione dei dati relativi ai dati sanitari. Di conseguenza i criteri di tale meccanismo dovranno essere adeguati a valutare i requisiti di protezione dei dati in tale settore.

73. ***[Esempio 4]***
Un meccanismo relativo alla certificazione dei trattamenti che prevedono sistemi di governance nell'ambito del trattamento dei dati dovrebbe identificare criteri che consentano il riconoscimento e la valutazione dei processi di governance e delle misure tecniche e organizzative a sostegno degli stessi.

74. ***[Esempio 5]***
I criteri di un meccanismo relativo al cloud computing dovranno tener conto degli speciali requisiti tecnici necessari per l'utilizzo dei servizi basati sul cloud. Se per esempio i server sono utilizzati al di fuori dell'UE i criteri dovranno tenere in considerazione le condizioni relative al trasferimento di dati personali verso paesi terzi stabilite al capo V del regolamento generale sulla protezione dei dati.

75. I criteri progettati per adattarsi a diversi oggetti di valutazione in diversi settori e/o Stati membri dovrebbero poter essere applicati a diversi contesti, consentire l'identificazione di misure idonee per l'adeguamento a trattamenti di piccola, media o grande entità e riflettere i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, in linea con il regolamento generale sulla protezione dei dati. Di conseguenza le procedure di certificazione (ad esempio riguardanti la documentazione, la verifica o il metodo e la profondità della valutazione) che integrano i criteri devono rispondere a tali esigenze e consentire la definizione e l'attuazione di regole, ad esempio per quanto riguarda l'applicazione dei criteri pertinenti ai singoli progetti di certificazione. I criteri devono permettere di valutare più facilmente se sono state fornite o meno garanzie sufficienti per l'attuazione di misure tecniche e organizzative adeguate.

6.3 PERIODO DI VALIDITÀ DEI CRITERI DI CERTIFICAZIONE

76. I criteri di certificazione devono essere affidabili nel tempo, ma non per questo dovrebbero essere immutabili. Una loro revisione dovrà essere effettuata per esempio in caso di:

- modifiche del quadro giuridico,
- interpretazione dei termini e delle condizioni nell'ambito di sentenze della Corte di giustizia dell'Unione europea, o
- avanzamento delle conoscenze tecnologiche di settore.

Per il Comitato europeo per la protezione dei dati
La presidente

(Andrea Jelinek)

ALLEGATO
COMPITI E POTERI DELLE AUTORITÀ DI CONTROLLO IN RELAZIONE ALLA CERTIFICAZIONE IN CONFORMITÀ DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

	Disposizioni	Prescrizioni
Compiti	Articolo 43, paragrafo 6	L'autorità di controllo è tenuta a rendere pubblici i criteri di cui all'articolo 42, paragrafo 5, in forma facilmente accessibile e a trasmetterli al Comitato.
	Articolo 57, paragrafo 1, lettera n)	L'autorità di controllo è tenuta ad approvare i criteri di certificazione a norma dell'articolo 42, paragrafo 5.
	Articolo 57, paragrafo 1, lettera o)	Ove applicabile (ossia qualora rilasci la certificazione), l'autorità di controllo è tenuta a effettuare un riesame periodico della certificazione rilasciata in conformità dell'articolo 42, paragrafo 7.
	Articolo 64, paragrafo 1, lettera c)	L'autorità di controllo è tenuta a comunicare il progetto di decisione al Comitato quando la decisione è finalizzata ad approvare i criteri per la certificazione di cui all'articolo 42, paragrafo 5.
Poteri	Articolo 58, paragrafo 1, lettera c)	L'autorità di controllo ha il potere di effettuare riesami delle certificazioni a norma dell'articolo 42, paragrafo 7.
	Articolo 58, paragrafo 2, lettera h)	L'autorità di controllo ha il potere di revocare la certificazione o ingiungere all'organismo di certificazione di revocare la certificazione oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione.
	Articolo 58, paragrafo 3, lettera e)	L'autorità di controllo ha il potere di accreditare gli organismi di certificazione.
	Articolo 58, paragrafo 3, lettera f)	L'autorità di controllo ha il potere di rilasciare certificazioni e approvare i criteri di certificazione.
	Articolo 58, paragrafo 3, lettera e)	L'autorità di controllo ha il potere di accreditare gli organismi di certificazione.
	Articolo 58, paragrafo 3, lettera f)	L'autorità di controllo ha il potere di rilasciare certificazioni e approvare i criteri di certificazione.

NOTE

[1] Punto 45.

[2] Gruppo di lavoro Articolo 29, parere 3/2010 sul principio di responsabilizzazione, WP173, 13 luglio 2010, punti da 69 a 71.

[3] Gruppo di lavoro Articolo 29, parere 3/2010 sul principio di responsabilizzazione, WP173, punto 69.

[4] Nell'ambito delle presenti linee guida il termine "meccanismi di certificazione" si riferisce collettivamente ai meccanismi di certificazione e ai sigilli e marchi di protezione dei dati, cfr. la sezione 1.3.2.

[5] Il considerando 100 rileva che dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione "che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi, al fine di migliorare la trasparenza e il rispetto del regolamento".

[6] Cfr. Gruppo di lavoro Articolo 29, Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) 2016/679 (WP253).

Linee guida 4/2018 relative all'accreditamento degli organismi di certificazione ai sensi dell'articolo 43 del regolamento generale sulla protezione dei dati (2016/679)

Adottate il 4 dicembre 2018

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

visto l'articolo 70, paragrafo 1, lettera e), del regolamento 2016/679/UE del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

Indice

1. INTRODUZIONE

Il regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679) («il RGPD»), entrato in vigore il 25 maggio 2018, istituisce un quadro di conformità aggiornato per la protezione dei dati in Europa, basato sul principio di responsabilizzazione e sulla tutela di diritti fondamentali. All'interno di tale nuovo quadro, risultano essenziali diverse misure intese a facilitare la conformità alle disposizioni del RGPD. Esse includono requisiti obbligatori in circostanze specifiche (inclusa la nomina di responsabili della protezione dei dati e lo svolgimento di valutazioni d'impatto sulla protezione dei dati) nonché misure volontarie, quali codici di condotta e meccanismi di certificazione.

Nell'ambito dell'istituzione di meccanismi di certificazione e di sigilli e marchi di protezione dei dati, l'articolo 43, paragrafo 1, del RGPD impone agli Stati membri di garantire che gli organismi di certificazione che rilasciano certificazioni ai sensi dell'articolo 42, paragrafo 1, siano accreditati dall'autorità di controllo competente o dall'organismo nazionale di accreditamento, o da entrambi. Se l'accreditamento è effettuato dall'organismo nazionale di accreditamento in conformità della norma ISO/IEC 17065/2012, devono essere applicati anche i requisiti aggiuntivi stabiliti dall'autorità di controllo competente.

Meccanismi di certificazione significativi possono migliorare la conformità al RGPD e la trasparenza per gli interessati e nelle relazioni tra imprese (B2B), ad esempio tra i titolari e i responsabili del trattamento. I titolari e i responsabili del trattamento dei dati beneficeranno di un'attestazione di terza parte che dimostra la conformità delle loro operazioni di trattamento[1].

In questo contesto, il comitato europeo per la protezione dei dati riconosce la necessità di fornire orientamenti in relazione all'accreditamento. Il valore e lo scopo peculiari dell'accreditamento consistono nell'attestazione autorevole della competenza degli organismi di certificazione, e ciò consente di creare fiducia nel meccanismo stesso di certificazione.
Le presenti linee-guida mirano a fornire indicazioni sull'interpretazione e l'attuazione delle disposizioni di cui all'articolo 43 del RGPD. In particolare, esse intendono aiutare gli Stati membri, le autorità di controllo e gli organismi nazionali di accreditamento a stabilire un quadro di riferimento coerente e armonizzato per l'accreditamento degli organismi di certificazione che rilasciano certificazioni in conformità del RGPD.

2. AMBITO DI APPLICAZIONE DELLE LINEE-GUIDA

Le presenti Linee-guida:

- definiscono l'obiettivo dell'accreditamento nel contesto del RGPD;
- illustrano le procedure disponibili per l'accreditamento degli organismi di certificazione a norma dell'articolo 43, paragrafo 1, e individuano le questioni fondamentali da prendere in considerazione;
- forniscono un quadro di riferimento per stabilire requisiti di accreditamento aggiuntivi quando l'accreditamento è gestito dall'organismo nazionale di accreditamento; e
- forniscono un quadro di riferimento per stabilire requisiti di accreditamento quando l'accreditamento è gestito dall'autorità di controllo.

Le linee-guida non costituiscono un manuale di procedure per l'accreditamento degli organismi di certificazione a norma del RGPD, né elaborano una nuova norma tecnica per l'accreditamento degli organismi di certificazione ai fini del RGPD.
Le presenti linee-guida sono rivolte ai seguenti soggetti:

- Stati membri, che devono garantire che gli organismi di certificazione siano accreditati dall'autorità di controllo e/o dall'organismo nazionale di accreditamento;
- organismi nazionali di accreditamento, che effettuano l'accreditamento degli organismi di certificazione a norma dell'articolo 43, paragrafo 1, lettera b);
- l'autorità di controllo competente, che specifica «requisiti aggiuntivi» rispetto a quelli di cui alla norma ISO/IEC 17065/2012[2], quando l'accreditamento è effettuato dall'organismo nazionale di accreditamento a norma dell'articolo 43, paragrafo 1, lettera b);
- il comitato europeo per la protezione dei dati, quando rilascia un parere e approva i requisiti di accreditamento dell'autorità di controllo competente, a norma dell'articolo 43, paragrafo 3, dell'articolo 70, paragrafo 1, lettera p) e dell'articolo 64, paragrafo 1, lettera c);
- l'autorità di controllo competente, che precisa i requisiti di accreditamento quando l'accreditamento è effettuato dall'autorità di controllo stessa, a norma dell'articolo 43, paragrafo 1, lettera a);

- altre parti interessate, quali i soggetti che si candidano a operare da organismi di certificazione o i proprietari di schemi di certificazione che definiscano criteri e procedure di certificazione[3].

DEFINIZIONI

Le seguenti definizioni mirano a promuovere un'interpretazione comune degli elementi fondamentali del processo di accreditamento. Devono essere considerate come punti di riferimento e non hanno alcuna pretesa di insindacabilità. Queste definizioni si basano sui quadri regolamentari e sulle norme esistenti, in particolare sulle disposizioni pertinenti del RGPD e della norma ISO/IEC 17065/2012.
Ai fini delle presenti linee-guida, si applicano le seguenti definizioni:

per *«accreditamento»* degli organismi di certificazione: si rimanda alla sezione 3 sull'interpretazione dell'accreditamento ai fini dell'articolo 43 del RGPD;

per *«requisiti aggiuntivi»* si intendono i requisiti stabiliti dall'autorità di controllo competente e sulla base dei quali viene eseguito l'accreditamento[4];

per *«certificazione»* si intende la valutazione e l'attestazione imparziale di terza parte[5] in merito al comprovato rispetto dei criteri di certificazione;

per *«organismo di certificazione»* si intende un organismo terzo di valutazione della conformità[6] che gestisce[7] un meccanismo di certificazione[8];

per *«schema di certificazione»* si intende un sistema di certificazione relativo a prodotti, processi e servizi specifici ai quali si applicano gli stessi requisiti specifici, norme e procedure specifiche[9];

per *«criteri»* o criteri di certificazione si intendono i criteri in base ai quali viene effettuata una certificazione (ossia, la valutazione della conformità)[10];

per *«organismo nazionale di accreditamento»* si intende l'unico organismo che in uno Stato membro è stato autorizzato da tale Stato a svolgere attività di accreditamento, a norma del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio[11].

3. INTERPRETAZIONE DI «ACCREDITAMENTO» AI FINI DELL'ARTICOLO 43 DEL RGPD

Il RGPD non fornisce una definizione di «accreditamento». L'articolo 2, paragrafo 10, del regolamento (CE) n. 765/2008, che stabilisce requisiti generali in materia di accreditamento, definisce l'accreditamento come segue:

«attestazione da parte di un organismo nazionale di accreditamento che certifica che un determinato organismo di valutazione della conformità soddisfa

i criteri stabiliti da norme armonizzate e, ove appropriato, ogni altro requisito supplementare, compresi quelli definiti nei rilevanti programmi settoriali, per svolgere una specifica attività di valutazione della conformità».
Ai sensi della norma ISO/IEC 17011

«l'accreditamento indica l'attestazione da parte di terzi recante prova formale che un determinato organismo di valutazione della conformità ha le competenze necessarie per svolgere specifiche attività di valutazione della conformità».

L'articolo 43, paragrafo 1, dispone quanto segue:

«Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 57 e 58, gli organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati, rilasciano e rinnovano la certificazione, dopo averne informato l'autorità di controllo al fine di consentire alla stessa di esercitare i suoi poteri a norma dell'articolo 58, paragrafo 2, lettera h), ove necessario. Gli Stati membri garantiscono che tali organismi di certificazione siano accreditati da uno o entrambi dei seguenti organismi:

(a) dall'autorità di controllo competente ai sensi degli articoli 55 o 56;
(b) dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio conformemente alla norma ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente ai sensi degli articoli 55 o 56».

Per quanto riguarda il RGPD, i requisiti di accreditamento si baseranno su:

- la norma ISO/IEC 17065/2012 e i «requisiti aggiuntivi» stabiliti dall'autorità di controllo competente ai sensi dell'articolo 43, paragrafo 1, lettera b), quando l'accreditamento è effettuato dall'organismo nazionale di accreditamento e dall'autorità di controllo, quando essa stessa effettua l'accreditamento.

In entrambi i casi, i requisiti consolidati devono includere i requisiti di cui all'articolo 43, paragrafo 2.

Il comitato europeo per la protezione dei dati riconosce che lo scopo dell'accreditamento è fornire una dichiarazione autorevole della competenza di un determinato organismo a svolgere attività di certificazione (attività di valutazione della conformità)[12]. Per accreditamento, ai sensi del RGPD, si intende quanto segue:

l'attestazione[13] da parte di un organismo nazionale di accreditamento e/o di un'autorità di controllo che un organismo di certificazione[14] è qualificato a effettuare la certificazione ai sensi degli articoli 42 e 43 del RGPD, tenendo conto della norma ISO/IEC 17065/2012 e dei requisiti aggiuntivi stabiliti dall'autorità di controllo e/o dal Comitato.

4. ACCREDITAMENTO AI SENSI DELL'ARTICOLO 43, PARAGRAFO 1, DEL RGPD

L'articolo 43, paragrafo 1, riconosce l'esistenza di diverse opzioni per l'accreditamento degli organismi di certificazione. Il RGPD impone alle autorità di controllo e agli Stati membri di definire il processo di accreditamento degli organismi di certificazione. In questa sezione sono indicate le modalità di accreditamento di cui all'articolo 43.

4.1 RUOLO DEGLI STATI MEMBRI

L'articolo 43, paragrafo 1, impone agli Stati membri di *garantire* che gli organismi di certificazione siano accreditati, ma consente a ciascuno Stato membro di determinare a chi spetti condurre la valutazione ai fini dell'accreditamento. Sulla base dell'articolo 43, paragrafo 1, sono disponibili tre opzioni; l'accreditamento è effettuato:

(1) esclusivamente dall'autorità di controllo, sulla base dei propri requisiti;
(2) esclusivamente dall'organismo nazionale di accreditamento, designato a norma del regolamento (CE) n. 765/2008 e in conformità della norma ISO/IEC 17065/2012 e dei requisiti aggiuntivi stabiliti dall'autorità di controllo competente; oppure
(3) sia dall'autorità di controllo che dall'organismo nazionale di accreditamento (e conformemente a tutti i requisiti di cui al precedente punto 2).

Spetta al singolo Stato membro decidere se tali attività di accreditamento dovranno essere svolte dall'organismo nazionale di accreditamento, dall'autorità di controllo o da entrambi, ma in ogni caso lo Stato membro dovrebbe garantire che siano messe a disposizione risorse idonee[15].

4.2 INTERAZIONE CON IL REGOLAMENTO (CE) N. 765/2008

Il comitato europeo per la protezione dei dati osserva che l'articolo 2, paragrafo 11, del regolamento (CE) n. 765/2008, definisce un organismo nazionale di accreditamento come «l'unico organismo che in uno Stato membro è stato autorizzato da tale Stato a svolgere attività di accreditamento».

L'articolo 2, paragrafo 11, potrebbe essere considerato in conflitto con l'articolo 43, paragrafo 1, del RGPD, che consente l'accreditamento da parte di un organismo diverso dall'organismo nazionale di accreditamento dello Stato membro. Il comitato europeo per la protezione dei dati ritiene che l'intenzione del legislatore UE sia stata quella di derogare al principio generale secondo cui l'accreditamento deve essere effettuato esclusivamente da un organismo nazionale di accreditamento, conferendo alle autorità di controllo lo stesso potere in materia di accreditamento degli organismi di certificazione. L'articolo 43, paragrafo 1, si caratterizza pertanto come lex specialis rispetto all'articolo 2, paragrafo 11, del regolamento (CE) n. 765/2008.

4.3 IL RUOLO DELL'ORGANISMO NAZIONALE DI ACCREDITAMENTO

L'articolo 43, paragrafo 1, lettera b), prevede che l'organismo nazionale di accreditamento accrediti gli organismi di certificazione conformemente alla norma ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente.

Per chiarezza, il comitato europeo per la protezione dei dati sottolinea che il riferimento specifico all'articolo 43, paragrafo 1, lettera b), nel testo del paragrafo 3 dello stesso articolo, implica che «tali requisiti» siano i «requisiti aggiuntivi» stabiliti dall'autorità di controllo competente ai sensi dell'articolo 43, paragrafo 1, lettera b), e i requisiti stabiliti all'articolo 43, paragrafo 2.

Nel processo di accreditamento, gli organismi nazionali di accreditamento applicano i requisiti aggiuntivi che devono essere forniti dalle autorità di controllo.

Un organismo di certificazione che sia già accreditato sulla base della norma ISO/IEC 17065/2012 per schemi di certificazione non relativi al RGPD, e che desideri estendere l'ambito del proprio accreditamento per includere la certificazione rilasciata in conformità del RGPD dovrà soddisfare i requisiti aggiuntivi stabiliti dall'autorità di controllo se l'accreditamento è gestito dall'organismo nazionale di accreditamento. Se l'accreditamento per la certificazione ai sensi del RGPD è offerto solo dall'autorità di controllo competente, un organismo di certificazione che faccia richiesta di accreditamento dovrà soddisfare i requisiti stabiliti dalla relativa autorità di controllo.

4.4 IL RUOLO DELL'AUTORITÀ DI CONTROLLO

Il comitato europeo per la protezione dei dati osserva che l'articolo 57, paragrafo 1, lettera q), stabilisce che l'autorità di controllo *effettua* l'accreditamento di un organismo di certificazione ai sensi dell'articolo 43 in quanto «compito dell'autorità di controllo» ai sensi dell'articolo 57; e l'articolo 58, paragrafo 3, lettera e), stabilisce che l'autorità di controllo ha il potere autorizzativo e consultivo per accreditare gli organismi di certificazione a norma dell'articolo 43. La formulazione dell'articolo 43, paragrafo 1, offre una certa flessibilità e la funzione di accreditamento dell'autorità di controllo dovrebbe essere interpretata come un compito non tassativo. La legislazione degli Stati membri potrà chiarire questo punto. Tuttavia, nel processo di accreditamento da parte di un organismo nazionale di accreditamento, l'articolo 43, paragrafo 2, lettera a), impone all'organismo di certificazione di dimostrare in modo convincente all'autorità di controllo competente la propria indipendenza e competenza in rapporto all'oggetto del meccanismo di certificazione che esso offre[16].

Se uno Stato membro stabilisce che gli organismi di certificazione devono essere accreditati dall'autorità di controllo, quest'ultima dovrebbe stabilire i requisiti per l'accreditamento, compresi, tra gli altri, i requisiti di cui all'articolo 43, paragrafo 2. Rispetto agli obblighi relativi all'accreditamento degli organismi

di certificazione da parte degli organismi nazionali di accreditamento, l'articolo 43 fornisce minori indicazioni in materia di requisiti per l'accreditamento nel caso in cui sia l'autorità di controllo stessa a effettuare l'accreditamento. Al fine di contribuire ad un approccio armonizzato all'accreditamento, i requisiti di accreditamento utilizzati dall'autorità di controllo dovrebbero basarsi sulla norma ISO/IEC 17065 ed essere integrati dai requisiti aggiuntivi stabiliti da tale autorità di controllo ai sensi dell'articolo 43, paragrafo 1, lettera b). Il comitato europeo per la protezione dei dati osserva che l'articolo 43, paragrafo 2, lettere da a) ad e), rispecchia e precisa i requisiti di cui alla norma ISO 17065, contribuendo così alla coerenza.

Se uno Stato membro stabilisce che gli organismi di certificazione devono essere accreditati dagli organismi nazionali di accreditamento, l'autorità di controllo dovrebbe stabilire requisiti aggiuntivi che integrano le convenzioni di accreditamento esistenti previste dal regolamento (CE) n. 765/2008 (i cui articoli da 3 a 14 riguardano l'organizzazione e il funzionamento dell'accreditamento degli organismi di valutazione della conformità) e le norme tecniche che descrivono i metodi e le procedure degli organismi di certificazione. Alla luce di ciò, il regolamento (CE) n. 765/2008 fornisce ulteriori indicazioni: l'articolo 2, paragrafo 10, definisce l'accreditamento e fa riferimento a «norme armonizzate» e a «ogni altro requisito supplementare, compresi quelli definiti nei rilevanti programmi settoriali». Ne consegue che i requisiti aggiuntivi stabiliti dall'autorità di controllo dovrebbero includere requisiti specifici ed essere incentrati sull'agevolazione della valutazione, tra l'altro, dell'indipendenza e del livello di competenza in materia di protezione dei dati degli organismi di certificazione - ad esempio la loro capacità di valutare e certificare le operazioni di trattamento dei dati personali da parte dei titolari e dei responsabili del trattamento ai sensi dell'articolo 42, paragrafo 1. Ciò include le competenze richieste per i programmi settoriali e per quanto riguarda la tutela dei diritti e delle libertà fondamentali delle persone fisiche e in particolare il loro diritto alla protezione dei dati personali[17]. L'allegato alle presenti linee-guida può aiutare le autorità di controllo competenti a stabilire i «requisiti aggiuntivi» ai sensi dell'articolo 43, paragrafo 1, lettera b), e dell'articolo 43, paragrafo 3.

L'articolo 43, paragrafo 6, stabilisce che «i requisiti di cui al paragrafo 3 del presente articolo e i criteri di certificazione di cui all'articolo 42, paragrafo 5, sono resi pubblici dall'autorità di controllo in una forma facilmente accessibile». Pertanto, per garantire la trasparenza, tutti i criteri e i requisiti approvati da un'autorità di controllo devono essere pubblicati. In termini di qualità e fiducia negli organismi di certificazione, sarebbe auspicabile che tutti i requisiti per l'accreditamento fossero facilmente accessibili al pubblico.

4.5 AUTORITÀ DI CONTROLLO CHE AGISCE IN QUALITÀ DI ORGANISMO DI CERTIFICAZIONE

L'articolo 42, paragrafo 5, stabilisce che un'autorità di controllo può rilasciare certificazioni, ma il RGPD non richiede che essa sia accreditata per soddisfare

i requisiti di cui al regolamento (CE) n. 765/2008. Il comitato europeo per la protezione dei dati osserva che l'articolo 43, paragrafo 1, lettera a), e in particolare l'articolo 58, paragrafo 2, lettera h), e paragrafo 3, lettere a), e) ed f), autorizzano le autorità di controllo a effettuare sia l'accreditamento che la certificazione e, allo stesso tempo, a fornire consulenza e, se del caso, a revocare le certificazioni o a ingiungere agli organismi di certificazione di non rilasciare certificazioni.

Vi possono essere situazioni in cui è opportuno o necessario garantire la separazione dei ruoli e delle funzioni di accreditamento e di certificazione, ad esempio qualora in uno Stato membro vi siano un'autorità di controllo e altri organismi di certificazione che rilascino la stessa tipologia di certificazioni. Le autorità di controllo dovrebbero pertanto adottare misure organizzative atte a mantenere distinti i compiti che il RGPD individua al fine di rendere solidi e facilitare i meccanismi di certificazione, evitando al tempo stesso possibili conflitti di interesse derivanti dall'esecuzione di tali compiti. Inoltre, gli Stati membri e le autorità di controllo dovrebbero tenere conto del livello di armonizzazione europeo al momento di formulare la legislazione e le procedure nazionali in materia di accreditamento e certificazione in conformità del RGPD.

4.6 REQUISITI DI ACCREDITAMENTO

L'allegato alle presenti linee-guida (*) fornisce indicazioni su come definire requisiti aggiuntivi di accreditamento. Individua le disposizioni pertinenti nel RGPD e suggerisce i requisiti che le autorità di controllo e gli organismi nazionali di accreditamento dovrebbero prendere in considerazione per garantire il rispetto del RGPD.

Come stabilito in precedenza, se gli organismi di certificazione sono accreditati dall'organismo nazionale di accreditamento ai sensi del regolamento (CE) n. 765/2008, la norma ISO/IEC 17065/2012 sarà la norma di accreditamento pertinente, integrata dai requisiti aggiuntivi stabiliti dall'autorità di controllo. L'articolo 43, paragrafo 2, rispecchia le disposizioni generali della norma ISO/IEC 17065/2012 alla luce della tutela dei diritti fondamentali ai sensi del RGPD. Il quadro di riferimento di cui all'allegato utilizza l'articolo 43, paragrafo 2, e la norma ISO/IEC 17065/2012 come base per l'individuazione dei requisiti, nonché ulteriori criteri relativi alla valutazione delle competenze in materia di protezione dei dati degli organismi di certificazione e della loro capacità di rispettare i diritti e le libertà delle persone fisiche con riguardo al trattamento dei dati personali, come sancito nel RGPD. Il comitato europeo per la protezione dei dati sottolinea la particolare attenzione prestata affinché sia garantito che gli organismi di certificazione dispongano di un livello adeguato di competenze riguardo alla protezione dei dati conformemente all'articolo 43, paragrafo 1.

(*) *NDR. L'allegato qui citato è stato adottato dall'EDPB successivamente al 25 maggio 2019.*

I requisiti aggiuntivi di accreditamento stabiliti dall'autorità di controllo si applicheranno a tutti gli organismi di certificazione che richiederanno l'accreditamento. L'organismo di accreditamento valuterà se tale organismo di certificazione sia competente a svolgere l'attività di certificazione in linea con i requisiti aggiuntivi e l'oggetto della certificazione. Si dovranno indicare i settori o le aree di certificazione specifici per i quali l'organismo di certificazione è accreditato.

Il comitato europeo per la protezione dei dati rileva, inoltre, che tale particolare competenza nel campo della protezione dei dati, oltre al rispetto dei requisiti della norma ISO/IEC 17065/2012, è richiesta anche qualora altri soggetti esterni, quali laboratori o auditor, svolgano parti o elementi di attività di certificazione per conto di un organismo di certificazione accreditato. In questi casi, non è previsto l'accreditamento di tali soggetti esterni ai sensi del RGPD stesso. Tuttavia, al fine di garantire l'idoneità di tali soggetti a svolgere attività per conto degli organismi di certificazione accreditati, è necessario che l'organismo di certificazione accreditato garantisca che anche il soggetto esterno disponga in modo dimostrabile delle competenze in materia di protezione dei dati richieste per l'organismo accreditato in relazione alla specifica attività svolta.

Il quadro per l'identificazione dei requisiti di accreditamento aggiuntivi presentato in allegato alle presenti linee-guida non costituisce un manuale di procedure ai fini dell'accreditamento effettuato dall'organismo nazionale di accreditamento o dall'autorità di controllo. Esso fornisce indicazioni strutturali e metodologiche alle autorità di controllo, offrendo pertanto una serie di strumenti per individuare i requisiti aggiuntivi ai fini dell'accreditamento.

Per il comitato europeo per la protezione dei dati
La presidente

(Andrea Jelinek)

NOTE

[1] Il considerando 100 del RGPD afferma che l'istituzione di meccanismi di certificazione può migliorare la trasparenza e il rispetto del regolamento e consentire agli interessati di valutare il livello di protezione dei dati dei relativi prodotti e servizi.

[2] Organizzazione internazionale per la standardizzazione: Valutazione della conformità - Requisiti per organismi che certificano prodotti, processi e servizi.

[3] GIl proprietario di uno schema di certificazione è un'organizzazione identificabile che ha stabilito i criteri di certificazione e i requisiti in base ai quali va valutata la conformità. L'accreditamento riguarda l'organismo che effettua le valutazioni della conformità (articolo 43, paragrafo 4) sulla base dei requisiti dello schema di certificazione e rilascia i relativi certificati (ossia l'organismo di certificazione, noto anche come organismo di valutazione della conformità). L'organismo che effettua le valutazioni potrebbe essere la stessa organizzazione che ha sviluppato lo schema di certificazione e ne è proprietaria, ma potrebbero sussistere accordi in base ai quali un'organizzazione è proprietaria dello schema e un'altra (o più di una) effettua le valutazioni.

[4] Articolo 43, paragrafi 1, 3 e 6.

[5] Si noti che, secondo la norma ISO 17000, l'attestazione di terza parte (certificazione) è "applicabile a tutti gli oggetti della valutazione della conformità" (5.5) "a eccezione degli organismi di valutazione della conformità stessi, ai quali è applicabile l'accreditamento" (5.6).

[6] L'attività di valutazione della conformità di terza parte è svolta da un'organizzazione indipendente dalla persona o dall'organizzazione che fornisce l'oggetto e da interessi da utilizzatore per l'oggetto stesso, cfr. ISO 17000, 2.4.

[7] Cfr. ISO 17000, 2.5: organismo che svolge servizi di valutazione della conformità; ISO 17011: organismo che svolge servizi di valutazione della conformità e che può essere oggetto di accreditamento; ISO 17065, 3.12.

[8] Articolo 42, paragrafi 1 e 5, del RGPD.

[9] Cfr. 3.9 in combinato disposto con l'allegato B della norma ISO 17065.

[10] Cfr. articolo 42, paragrafo 5.

[11] Cfr. articolo 2, punto 11, del regolamento n. 765/2008/CE.

[12] Cfr. considerando 15 del regolamento n. 765/2008/CE.

[13] Cfr. articolo 2, punto 10, del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti.

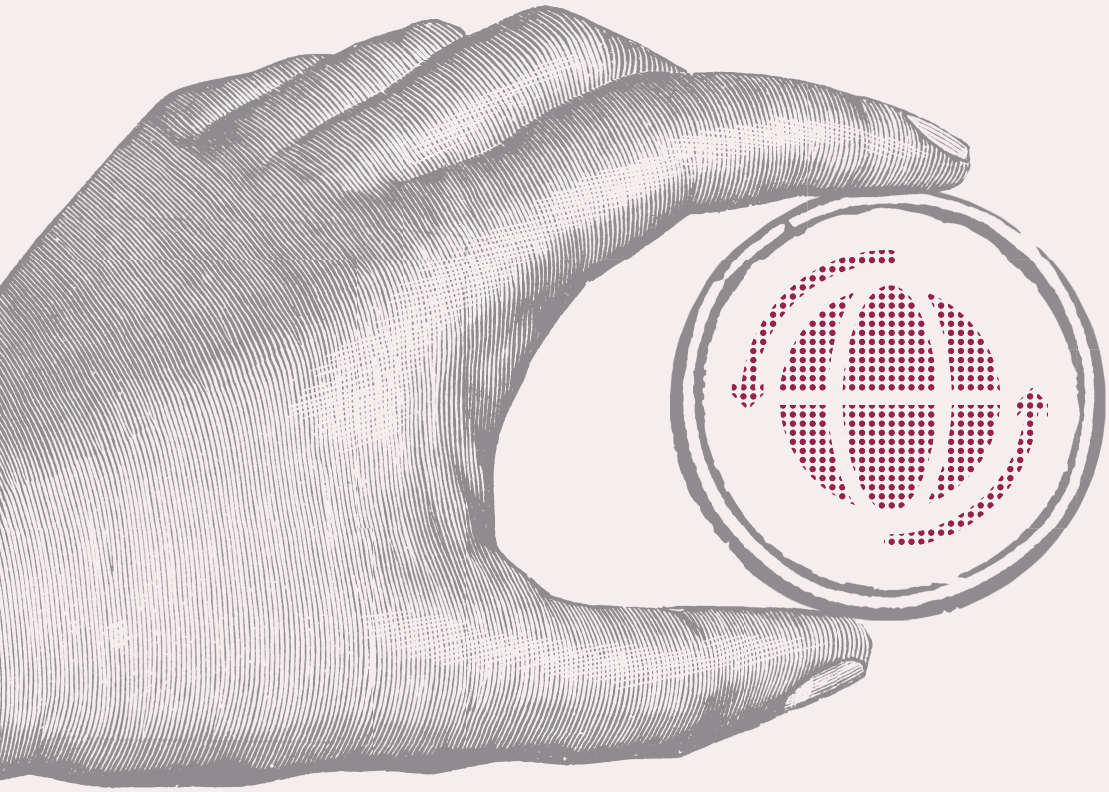
[14] Cfr. la definizione del termine «accreditamento» ai sensi della norma ISO 17011.

[15] Cfr. articolo 4, paragrafo 9, del regolamento (CE) n. 765/2008.

[16] I requisiti aggiuntivi stabiliti dall'autorità di controllo ai sensi dell'articolo 43, paragrafo 1, lettera b), dovrebbero specificare i requisiti in materia di indipendenza e di competenza. Cfr. anche allegato 1 delle presenti Linee-guida.

[17] Articolo 1, paragrafo 2, del RGPD.

3 Trasferimenti di dati verso paesi terzi e organismi internazionali



Premessa
Trasferimenti di dati verso paesi terzi e organismi internazionali

Il GDPR non ha modificato l'approccio della direttiva e del Codice privacy rispetto ai trasferimenti di dati personali verso Paesi terzi. Mentre, infatti, vige la più assoluta libertà di circolazione dei dati personali all'interno dell'Ue e dello spazio economico europeo, posti sotto l'egida del GDPR, il trasferimento dei dati al di fuori dei confini dell'Ue è vietato a meno che il titolare possa far valere specifiche garanzie. Tuttavia, il GDPR chiarisce l'ordine di importanza di tali garanzie e introduce, al tempo stesso, nuovi strumenti per consentire ai titolari di procedere ai trasferimenti (come la certificazione o l'adesione a un codice di condotta). Più in generale, il GDPR ha reso maggiormente stringenti i requisiti che devono essere soddisfatti qualunque sia lo strumento di garanzia utilizzato per i trasferimenti di dati verso Paesi terzi, anche alla luce delle sentenze con cui negli ultimi venti anni la Corte di giustizia dell'Ue ha precisato i contorni della tutela che deve essere assicurata a ogni dato personale quando lascia il territorio di uno Stato membro dell'Ue.

L'adeguatezza del Paese terzo di destinazione è la prima delle garanzie in questione, alla quale il GDPR attribuisce chiaramente preminenza perché in grado di tutelare a 360 gradi il dato personale trasferito: in questi casi la tutela è offerta, infatti, dal sistema-Paese nel suo complesso, cioè dall'insieme dalla sua legislazione, delle prassi, dei meccanismi di ricorso giudiziario o amministrativo. Tuttavia, il sistema-Paese di destinazione dei dati deve garantire, a questo scopo, un livello di tutela "sostanzialmente equivalente" a quello dello Stato membro di provenienza. In merito, i Garanti europei hanno chiarito come il GDPR rafforzi ed estenda i requisiti dell'adeguatezza (equivalenza sostanziale), con un documento comparativo dove sono sottolineati gli elementi di cui la Commissione europea (incaricata di decidere se un Paese terzo garantisca questa tutela "adeguata", su parere favorevole del Comitato europeo per la protezione dei dati) dovrà tenere conto.

Un'ulteriore serie di importanti documenti elaborati in questo ambito dal WP29 riguarda un altro strumento che può offrire, ai sensi del GDPR, garanzie

di tutela del dato trasferito ove non vi sia un riconoscimento di adeguatezza di uno o più Paesi terzi, ossia le cosiddette "norme vincolanti di impresa" – che rappresentano, in sostanza, policy di gruppo aziendale nelle quali sono elencati i principi e i meccanismi con cui i dati circolano e sono trattati all'interno di tale gruppo multinazionale nel rispetto del GDPR. L'Articolo 47 di quest'ultimo ha sancito i contenuti e i requisiti che devono essere assicurati nel redigere le norme vincolanti d'impresa, sulla base dell'esperienza applicativa maturata in questi anni dalle Autorità di protezione dati nel dialogo con molte grandi aziende multinazionali. Il WP29 ha voluto, dunque, da un lato chiarire quali siano gli elementi e i principi che devono figurare, oggi, nelle norme vincolanti d'impresa e, dall'altro, come si modifichino le procedure di cooperazione fra Autorità di controllo nazionali ai fini dell'approvazione di tali norme (compreso un meccanismo pratico di individuazione dell'Autorità "competente" a decidere in materia, tenuto conto dei nuovi criteri di competenza introdotti dal GDPR), nonché quali informazioni le aziende debbano evidenziare nel rivolgere all'Autorità competente una richiesta di approvazione delle loro policy vincolanti d'impresa.

Fondamentali, infine, le linee-guida interpretative delle disposizioni dell'Art. 49 del GDPR, in cui sono elencati i presupposti che, in deroga al divieto generale di trasferimento e in assenza di ogni altra garanzia prevista dal GDPR, i titolari possono utilizzare per trasferire dati verso Paesi terzi: consenso esplicito della persona interessata, adempimento di obblighi contrattuali nei confronti dell'interessato, interesse vitale dell'interessato o di terzi, ecc. . Si tratta dell'ultimo gradino nell'ideale gerarchia delle fonti sopra delineata, in cui l'adeguatezza del Paese terzo occupa il primo posto. Le linee-guida chiariscono, in via generale, che l'applicazione di questi presupposti deve avvenire necessariamente in chiave restrittiva, trattandosi di deroghe e in considerazione dell'assenza di qualsivoglia ulteriore tutela per i dati personali una volta trasferiti nel Paese terzo. Soprattutto, i Garanti chiariscono che non può trattarsi di trasferimenti massivi, sistematici o ripetitivi, per i quali occorre ricorrere alle altre garanzie sopra ricordate, e forniscono numerosi esempi di situazioni nelle quali l'uno o l'altro dei presupposti in deroga fissati all'art. 49 si prestano o meno a essere utilizzati per trasferire informazioni al di fuori dell'Ue.

Criteri di riferimento per l'adeguatezza [WP 254 rev. 01]

Adottati il 28 novembre 2017
Versione emendata e adottata il 6 febbraio 2018

Il Gruppo è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della direzione generale Giustizia e consumatori, Commissione europea, B-1049 Bruxelles, Belgio, ufficio MO-59 05/35.

Sito web: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

INTRODUZIONE

Il Gruppo di lavoro per la protezione dei dati[1] ("Gruppo") ha già presentato un documento di lavoro sui trasferimenti di dati personali verso paesi terzi (WP12)[2]. In seguito all'entrata in vigore del regolamento generale dell'UE sulla protezione dei dati ("regolamento")[3], che ha sostituito la direttiva, il Gruppo sta rivedendo il documento WP12, contenente i suoi precedenti orientamenti, per aggiornarlo alla luce della nuova legislazione e della giurisprudenza recente della Corte di giustizia dell'Unione europea ("Corte")[4].

Il presente documento di lavoro si prefigge di aggiornare il capitolo 1 del WP12, relativo alla questione centrale del livello adeguato di protezione dei dati in un paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo o un'organizzazione internazionale (di seguito: "paesi terzi o organizzazioni internazionali"). Nei prossimi anni il documento sarà sottoposto a continue revisioni e, se necessario, aggiornato sulla base dell'esperienza pratica maturata grazie all'applicazione del regolamento. I capitoli 2 (*Applicazione dei principi ai paesi che hanno ratificato la convenzione n. 108 del Consiglio d'Europa*) e 3 (*Applicazione dei principi all'autodisciplina settoriale*) del documento WP12 dovrebbero essere aggiornati in una fase successiva.

Il presente documento di lavoro riguarda soltanto le decisioni di adeguatezza, che sono atti di esecuzione[5] della Commissione europea a norma dell'articolo 45 del regolamento. Altri aspetti dei trasferimenti di dati personali verso paesi terzi e organizzazioni internazionali saranno esaminati in successivi documenti di lavoro che saranno pubblicati separatamente (norme vincolanti d'impresa, deroghe).

Il presente documento mira a fornire orientamenti alla Commissione europea e al Gruppo, nel quadro del regolamento, per quanto concerne la valutazione del livello di tutela dei dati nei paesi terzi e nelle organizzazioni internazionali, stabilendo i principi fondamentali per la protezione dei dati che devono essere presenti nella legislazione di un paese terzo o in un'organizzazione internazionale per garantire un'equivalenza sostanziale con il quadro dell'UE. Inoltre, può fornire orientamenti ai paesi terzi e alle organizzazioni internazionali interessati a ottenere l'adeguatezza. Tuttavia, i principi delineati nel presente documento di lavoro non sono direttamente rivolti ai titolari del trattamento o ai responsabili del trattamento.

Il presente documento consta di 4 capitoli:

Capitolo 1: Alcune informazioni generali sul concetto di adeguatezza.

Capitolo 2: Aspetti procedurali per i riscontri relativi all'adeguatezza a norma del regolamento.

Capitolo 3: Principi generali di protezione dei dati. Questo capitolo contiene i principi generali fondamentali di protezione dei dati per garantire che il livello

di protezione dei dati in un paese terzo o un'organizzazione internazionale sia sostanzialmente equivalente a quello stabilito dalla legislazione dell'UE.

Capitolo 4: Garanzie sostanziali per l'accesso a fini di contrasto e di sicurezza nazionale allo scopo di limitare le ingerenze nei diritti fondamentali. Il capitolo riporta le garanzie sostanziali per l'accesso a fini di contrasto e di sicurezza nazionale alla luce della sentenza Schrems del 2015 della Corte e sulla base del documento di lavoro sulle garanzie sostanziali adottato dal Gruppo nel 2016.

CAPITOLO 1: ALCUNE INFORMAZIONI GENERALI SUL CONCETTO DI ADEGUATEZZA

L'articolo 45, paragrafo 1, del regolamento stabilisce il principio che i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale sono ammessi soltanto se il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato.

Questo concetto di "livello di protezione adeguato", che era già presente nella direttiva 95/46, è stato ulteriormente sviluppato dalla Corte. A questo proposito è importante richiamare il principio stabilito dalla Corte nella causa Schrems, secondo cui il "*livello di protezione*" nel paese terzo deve essere "*sostanzialmente equivalente*" a quello garantito all'interno dell'Unione, ma "*gli strumenti dei quali tale paese terzo si avvale, al riguardo, per assicurare un siffatto livello di protezione, possono essere diversi da quelli attuati all'interno dell'Unione*"[6]. Pertanto, l'obiettivo non è riprodurre punto per punto la legislazione europea, bensì stabilire i requisiti sostanziali - di base - di tale legislazione.

Scopo delle decisioni di adeguatezza da parte della Commissione europea è confermare formalmente con effetto vincolante per gli Stati membri[7] che il livello di protezione dei dati in un paese terzo o in un'organizzazione internazionale è sostanzialmente equivalente al livello di protezione dei dati all'interno dell'Unione europea[8]. L'adeguatezza può essere conseguita anche attraverso una combinazione di diritti degli interessati e obblighi in capo a chi effettua il trattamento o esercita il controllo sul trattamento, e il controllo da parte di organismi indipendenti. Le norme in materia di protezione dei dati, tuttavia, sono efficaci solo se sono azionabili e sono rispettate nella pratica. È pertanto necessario considerare non solo il contenuto delle norme applicabili ai dati personali trasferiti in un paese terzo o un'organizzazione internazionale, ma anche il sistema in atto per garantirne l'efficacia. La presenza di meccanismi di applicazione efficienti è di fondamentale importanza per garantire l'efficacia delle norme sulla protezione dei dati.

L'articolo 45, paragrafo 2, del regolamento stabilisce gli elementi che la Commissione europea deve prendere in considerazione nel valutare l'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale.

Per esempio, la Commissione deve prendere in considerazione lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione, l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti e gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale.

È chiaro dunque che qualsiasi analisi significativa dell'adeguatezza della protezione deve comprendere due elementi fondamentali: il contenuto delle norme applicabili e i mezzi per garantirne l'effettiva applicazione. Spetta alla Commissione europea verificare sistematicamente che le norme in vigore siano efficaci nella pratica.

Il "nucleo" dei principi di contenuto in materia di protezione dei dati e delle prescrizioni di "procedura/applicazione", la cui osservanza potrebbe essere considerata una condizione minima di adeguatezza della protezione, è tratto dalla Carta dei diritti fondamentali dell'Unione europea e dal regolamento. È inoltre opportuno prendere in considerazione altri accordi internazionali in materia di protezione dei dati, per esempio la convenzione n. 108[9].

Occorre prestare attenzione altresì al quadro giuridico per l'accesso delle autorità pubbliche ai dati personali. Ulteriori orientamenti in materia sono reperibili nel documento di lavoro 237 (il documento sulle garanzie sostanziali)[10] sulle garanzie nel contesto della sorveglianza.

Le disposizioni generali sulla protezione dei dati e la vita privata nel paese terzo non sono sufficienti. Nel quadro giuridico del paese terzo o dell'organizzazione internazionale devono figurare disposizioni specifiche che rispondono a necessità concrete correlate ad aspetti pratici rilevanti del diritto alla protezione dei dati. Tali disposizioni devono essere vincolanti.

CAPITOLO 2: ASPETTI PROCEDURALI PER I RISCONTRI RELATIVI ALL'ADEGUATEZZA A NORMA DEL REGOLAMENTO

Per poter adempiere al proprio compito di fornire consulenza alla Commissione europea a norma dell'articolo 70, paragrafo 1, lettera s), del regolamento, il comitato europeo per la protezione dei dati ("comitato") deve ricevere la documentazione necessaria, compresa la corrispondenza pertinente e le conclusioni tratte dalla Commissione europea. Se il quadro giuridico è complesso, dovrebbero essere fornite anche eventuali relazioni sul livello di protezione dei dati nel paese terzo o nell'organizzazione internazionale. In ogni caso, le informazioni fornite dalla Commissione europea dovrebbero essere esaustive e permettere al comitato di effettuare la valutazione del livello di protezione dei dati nel paese terzo. Il comitato fornirà in tempo utile un parere sui riscontri della Commissione europea e individuerà eventuali carenze nel quadro giuridico in materia di adeguatezza. Il comitato inoltre si adopererà per proporre variazioni o modifiche per ovviare alle eventuali carenze.

A norma dell'articolo 45, paragrafo 4, del regolamento, spetta alla Commissione controllare su base continuativa gli sviluppi che potrebbero incidere sul funzionamento delle decisioni di adeguatezza.

L'articolo 45, paragrafo 3, del regolamento stabilisce che deve essere effettuato un riesame periodico almeno ogni quattro anni. Si tratta di un'indicazione temporale generica, che deve essere adattata a ciascun paese terzo o a ciascuna organizzazione internazionale tramite una decisione di adeguatezza. A seconda delle circostanze particolari del caso, potrebbe essere giustificata una frequenza più breve. Inoltre, un incidente o nuove informazioni sul quadro giuridico del paese terzo o dell'organizzazione internazionale o una modifica dello stesso potrebbero rendere necessario anticipare il riesame rispetto al previsto. Sarebbe inoltre opportuno procedere tempestivamente a un primo riesame di una decisione di adeguatezza interamente nuova e adattare progressivamente il ciclo di riesame in base all'esito di tale attività.

Alla luce dell'obbligo del comitato di fornire alla Commissione un parere per valutare se il paese terzo, il territorio o uno o più settori specifici all'interno di tale paese terzo, o l'organizzazione internazionale non assicurino più un livello adeguato di protezione, il comitato deve ricevere a tempo debito dalla Commissione europea informazioni significative sul monitoraggio degli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale in questione. Il comitato dovrebbe quindi essere tenuto informato su eventuali processi di riesame e missioni di valutazione in corso nel paese terzo o con riferimento all'organizzazione internazionale. Il comitato apprezzerebbe un invito a partecipare a tali processi di riesame e missioni di valutazione.

Va inoltre rilevato che, a norma dell'articolo 45, paragrafo 5, del regolamento, la Commissione europea ha il diritto di revocare, modificare o sospendere le decisioni di adeguatezza in vigore. La procedura per revocare, modificare o sospendere le decisioni di adeguatezza dovrebbe conseguentemente coinvolgere il comitato, cui dovrebbe essere richiesto un parere a norma dell'articolo 70, paragrafo 1, lettera s).

In aggiunta, come ora previsto dall'articolo 58, paragrafo 5, del regolamento e in base a quanto stabilito dalla sentenza Schrems della Corte, le autorità di protezione dei dati devono poter intentare un'azione legale ove ritengano fondate le censure sollevate da una persona nei confronti di una decisione di adeguatezza: *"[...] incombe al legislatore nazionale prevedere mezzi di ricorso che consentano all'autorità nazionale di controllo di cui trattasi di far valere le censure che essa reputa fondate dinanzi ai giudici nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di tale autorità in ordine alla validità della decisione della Commissione, ad un rinvio pregiudiziale inteso all'esame della validità di tale decisione"*[11].

CAPITOLO 3: PRINCIPI GENERALI DI PROTEZIONE DEI DATI PER GARANTIRE CHE IL LIVELLO DI PROTEZIONE IN UN PAESE TERZO, UN TERRITORIO O UNO O PIÙ SETTORI SPECIFICI ALL'INTERNO DI TALE PAESE TERZO, O IN UN'ORGANIZZAZIONE INTERNAZIONALE SIA SOSTANZIALMENTE EQUIVALENTE A QUELLO GARANTITO DALLA LEGISLAZIONE DELL'UE

Il sistema di un paese terzo o di un'organizzazione internazionale deve contenere i seguenti principi di contenuto e meccanismi di procedura/applicazione basilari:

A. PRINCIPI DI CONTENUTO:

1) NOZIONI

Dovrebbero essere presenti nozioni e/o principi basilari in materia di protezione dei dati. Tali nozioni e principi non devono necessariamente riprendere la terminologia del regolamento, ma dovrebbero rispecchiare ed essere coerenti con le nozioni racchiuse nel diritto europeo in materia di protezione dei dati. A titolo esemplificativo, il regolamento contiene le seguenti nozioni fondamentali: "dati personali", "trattamento di dati personali", "titolare del trattamento", "responsabile del trattamento", "destinatario" e "dati sensibili".

2) CRITERI DI LICEITÀ E CORRETTEZZA DEL TRATTAMENTO PER FINI LEGITTIMI

I dati devono essere trattati in modo lecito, corretto e legittimo.
Le basi di legittimità che consentono il trattamento lecito, corretto e legittimo dei dati personali dovrebbero essere definite in maniera sufficientemente chiara. Il quadro europeo riconosce alcuni criteri di legittimità tra cui, per esempio, le disposizioni del diritto nazionale, il consenso dell'interessato, l'esecuzione di un contratto o il legittimo interesse del titolare del trattamento o di un terzo a condizione che non prevalgano gli interessi dell'interessato.

3) IL PRINCIPIO DELLA FINALITÀ LIMITATA

I dati dovrebbero essere trattati per una finalità specifica e successivamente utilizzati soltanto nella misura in cui non vi sia incompatibilità con la finalità del trattamento.

4) IL PRINCIPIO DELLA QUALITÀ E DELLA PROPORZIONALITÀ

I dati dovrebbero essere precisi e aggiornati laddove necessario. I dati dovrebbero essere adeguati, pertinenti e non eccedenti rispetto alle finalità perseguite.

5) IL PRINCIPIO DELLA CONSERVAZIONE DEI DATI

Di norma i dati dovrebbero essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

6) IL PRINCIPIO DELLA SICUREZZA E DELLA RISERVATEZZA

Qualsiasi organismo incaricato del trattamento dei dati dovrebbe assicurare che questi siano trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. Il livello di sicurezza dovrebbe tenere in considerazione lo stato dell'arte e i relativi costi.

7) IL PRINCIPIO DI TRASPARENZA

Ogni persona dovrebbe essere informata in merito a tutti i principali elementi del trattamento dei dati personali che la riguardano in forma chiara, facilmente accessibile, concisa, trasparente e di facile comprensione. Tali informazioni dovrebbero includere la finalità del trattamento, l'identità del titolare del trattamento, i diritti di cui gode e altre informazioni, purché ciò sia necessario a garantire la correttezza. A determinate condizioni, sono ammesse alcune eccezioni a tale diritto di informazione, ad esempio per salvaguardare le indagini penali, la sicurezza nazionale, l'indipendenza della magistratura e dei procedimenti giudiziari o altri importanti obiettivi di interesse pubblico generale, come nel caso dell'articolo 23 del regolamento.

8) I DIRITTI DI ACCESSO, RETTIFICA, CANCELLAZIONE E OPPOSIZIONE

L'interessato dovrebbe avere il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e l'accesso a tali dati, compresa una copia di tutti i dati trattati che lo riguardano.

L'interessato dovrebbe avere il diritto di ottenere la rettifica dei dati che lo riguardano, per motivi specifici, ad esempio ove siano palesemente inesatti o incompleti, nonché la loro cancellazione, ad esempio quando il trattamento non è più necessario o è illecito.

L'interessato dovrebbe inoltre avere il diritto di opporsi in qualsiasi momento, per motivi legittimi cogenti relativi alla sua situazione particolare, al trattamento dei dati che lo riguardano a determinate condizioni previste dalla legislazione del paese terzo. Il regolamento, ad esempio, prevede tra tali condizioni il caso in cui il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento o il caso in cui il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi.

L'esercizio di tali diritti non dovrebbe essere eccessivamente oneroso per l'interessato. Si potrebbero prevedere eventuali limitazioni a tali diritti, ad esempio per salvaguardare le indagini penali, la sicurezza nazionale, l'indipendenza della magistratura e dei procedimenti giudiziari o altri importanti obiettivi di interesse pubblico generale, come nel caso dell'articolo 23 del regolamento.

9) RESTRIZIONI AI TRASFERIMENTI SUCCESSIVI

Ulteriori trasferimenti dei dati personali da parte del destinatario del primo trasferimento dovrebbero essere consentiti soltanto quando anche il secondo destinatario (ossia il destinatario del trasferimento successivo) è soggetto a norme (comprese le norme contrattuali) che assicurano un livello di protezione adeguato e prevedono il rispetto delle istruzioni pertinenti durante il trattamento dei dati per conto del titolare del trattamento. Il livello di tutela delle persone fisiche i cui dati sono trasferiti non deve essere compromesso dal trasferimento successivo. Spetta al primo destinatario dei dati trasferiti dall'UE assicurare che siano previste garanzie adeguate per i trasferimenti successivi dei dati in mancanza di una decisione di adeguatezza. Tali trasferimenti successivi di dati dovrebbero essere possibili soltanto per finalità determinate e limitate e purché sussista una base giuridica per il trattamento.

B. ESEMPI DI PRINCIPI DI CONTENUTO SUPPLEMENTARI DA APPLICARE IN CASI SPECIFICI DI TRATTAMENTO:

1) CATEGORIE PARTICOLARI DI DATI

Dovrebbero esistere garanzie specifiche nel caso in cui siano interessate "categorie particolari" di dati[12]. Tali categorie dovrebbero riflettere quelle previste agli articoli 9 e 10 del regolamento. La protezione dovrebbe essere messa in atto tramite l'introduzione di requisiti di trattamento più severi, ad esempio il fatto che l'interessato fornisca il suo consenso esplicito al trattamento o tramite misure di sicurezza supplementari.

2) MARKETING DIRETTO

Se il trattamento dei dati avviene per finalità di marketing diretto, l'interessato dovrebbe essere in grado, in qualsiasi momento e gratuitamente, di opporsi a tale trattamento con riferimento ai dati che lo riguardano.

3) PROCESSO DECISIONALE AUTOMATIZZATO, COMPRESA LA PROFILAZIONE

Le decisioni basate unicamente sul trattamento automatizzato (processo decisionale automatizzato relativo alle persone fisiche), compresa la profilazione,

che producono effetti giuridici che riguardano l'interessato o incidono significativamente sulla sua persona sono ammesse soltanto a determinate condizioni stabilite dal quadro giuridico del paese terzo. Nel quadro europeo tali condizioni comprendono, per esempio, la necessità di ottenere il consenso esplicito dell'interessato o la necessità di tale decisione per la conclusione di un contratto. Se la decisione non è conforme alle condizioni stabilite dal quadro giuridico del paese terzo, l'interessato dovrebbe avere il diritto di non essere sottoposto alle sue prescrizioni. Il diritto del paese terzo dovrebbe, in ogni caso, prevedere le necessarie garanzie, compreso il diritto a essere informato sui motivi particolari sottesi alla decisione e sulla sua logica, a rettificare informazioni inaccurate o incomplete e a contestare la decisione qualora questa sia stata adottata sulla base di un fondamento di fatto errato.

C. MECCANISMI DI PROCEDURA E APPLICAZIONE

Anche se gli strumenti dei quali il paese terzo si avvale per assicurare un livello di protezione adeguato possono essere diversi da quelli attuati all'interno dell'Unione europea[13], un sistema coerente con quello europeo deve essere caratterizzato dalla presenza dei seguenti elementi:

1) AUTORITÀ DI CONTROLLO COMPETENTI INDIPENDENTI

Nel paese terzo dovrebbero essere presenti una o più autorità di controllo indipendenti, con il compito di monitorare, garantire e far rispettare le disposizioni in materia di protezione dei dati e della vita privata. L'autorità di controllo agisce in piena indipendenza e imparzialità nell'adempimento dei suoi compiti e nell'esercizio dei suoi poteri, senza richiedere né accettare istruzioni. In tale contesto, l'autorità di controllo dovrebbe disporre di tutti i necessari poteri e incarichi disponibili per garantire la conformità ai diritti in materia di protezione dei dati e per sensibilizzare l'opinione pubblica al riguardo. Dovrebbero inoltre essere presi in considerazione il personale e il bilancio dell'autorità di controllo. L'autorità di controllo dovrebbe essere in grado, infine, di condurre indagini di propria iniziativa.

2) IL SISTEMA DI PROTEZIONE DEI DATI DEVE GARANTIRE UN BUON LIVELLO DI CONFORMITÀ

Il sistema di un paese terzo dovrebbe garantire un buon livello di responsabilizzazione e di consapevolezza dei propri obblighi, compiti e responsabilità tra i titolari del trattamento e tra chi si occupa, per conto loro, del trattamento dei dati personali, e dei propri diritti e dei mezzi a disposizione per l'esercizio degli stessi tra gli interessati. L'esistenza di sanzioni effettive e dissuasive può svolgere un ruolo importante nel garantire il rispetto delle norme, così come la presenza di sistemi di verifica diretta da parte di autorità, ispettori o addetti indipendenti alla protezione dei dati.

3) RESPONSABILIZZAZIONE

Il quadro giuridico per la protezione dei dati di un paese terzo dovrebbe obbligare i titolari del trattamento e/o i soggetti che trattano i dati personali per loro conto a rispettarne le disposizioni e a fornire le prove di tale conformità, in particolare all'autorità di controllo competente. Tali misure potrebbero comprendere, per esempio, valutazioni dell'impatto della protezione dei dati, la tenuta di registri o file di log delle attività di trattamento dei dati per un periodo di tempo adeguato, la nomina di un addetto alla protezione dei dati o la protezione dei dati fin dalla progettazione e la protezione dei dati di default.

4) IL SISTEMA DI PROTEZIONE DEI DATI DEVE FORNIRE AIUTO E SOSTEGNO AGLI INTERESSATI NELL'ESERCIZIO DEI LORO DIRITTI NONCHÉ MECCANISMI DI RICORSO APPROPRIATI

L'interessato dovrebbe essere in grado di avvalersi di mezzi di ricorso per far valere i propri diritti con rapidità ed efficacia, e senza costi proibitivi, nonché per garantire la conformità. A tal fine devono essere disponibili meccanismi di controllo che consentano un'indagine indipendente sulle denunce e che permettano di individuare e sanzionare nella pratica eventuali violazioni del diritto alla protezione dei dati e al rispetto della vita privata.

In caso di inosservanza delle norme, all'interessato dovrebbe inoltre essere riconosciuto un mezzo di ricorso effettivo in sede amministrativa e giudiziale, anche ai fini del risarcimento per i danni subiti a causa di un trattamento illecito dei dati personali che lo riguardano. Si tratta di un elemento fondamentale che deve prevedere un sistema di valutazione o arbitrato indipendenti che permettano il pagamento di un risarcimento e l'imposizione di sanzioni, se del caso.

CAPITOLO 4: GARANZIE SOSTANZIALI NEI PAESI TERZI PER L'ACCESSO A FINI DI CONTRASTO E DI SICUREZZA NAZIONALE ALLO SCOPO DI LIMITARE LE INGERENZE NEI DIRITTI FONDAMENTALI

A norma dell'articolo 45, paragrafo 2, lettera a), del regolamento, nel valutare l'adeguatezza del livello di protezione la Commissione prende in considerazione "*la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione [...]*".
La Corte, nella sentenza Schrems, ha osservato che "*l'espressione 'livello di protezione adeguato' deve essere intesa nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza della direttiva 95/46, letta alla luce della Carta*". Anche se gli strumenti dei quali il paese terzo si avva-

le, al riguardo, possono essere diversi da quelli attuati all'interno dell'Unione, tali strumenti devono cionondimeno rivelarsi efficaci nella prassi[14].

A tale proposito, la Corte ha anche osservato in tono critico che la precedente decisione "Safe Harbor" "*non contiene alcuna dichiarazione quanto all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione verso gli Stati Uniti, ingerenze che entità statali di tale paese sarebbero autorizzate a compiere laddove perseguano obiettivi legittimi, come la sicurezza nazionale*".

Il Gruppo ha individuato nel parere WP237, adottato il 13 aprile 2016, garanzie sostanziali che rispecchiano la giurisprudenza della Corte e della CEDU in tema di controlli. Se è vero che le raccomandazioni formulate nel parere WP237 rimangono valide, e dovrebbero essere prese in considerazione nel valutare l'adeguatezza di un paese terzo per quanto concerne i controlli, altrettanto certo è che l'applicazione di tali garanzie può differire nei settori dell'accesso ai dati a fini di contrasto e di sicurezza nazionale. Tuttavia, per accedere ai dati a fini di contrasto o di sicurezza nazionale tutti i paesi terzi devono rispettare le seguenti quattro garanzie per essere considerati adeguati:

1) IL TRATTAMENTO DOVREBBE ESSERE FONDATO SU NORME CHIARE, PRECISE E ACCESSIBILI (BASE GIURIDICA)

2) È NECESSARIO DIMOSTRARE LA NECESSITÀ E LA PROPORZIONALITÀ DEGLI OBIETTIVI LEGITTIMI PERSEGUITI

3) IL TRATTAMENTO DEVE ESSERE SOTTOPOSTO A CONTROLLI INDIPENDENTI

4) GLI INTERESSATI DEVONO AVERE A DISPOSIZIONE MEZZI DI RICORSO EFFETTIVI

NOTE

[1] Istituito in virtù dell'articolo 29 della direttiva 95/46/CE relativa alla tutela dei dati.

[2] WP12 "Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati", adottato dal Gruppo il 24 luglio 1998.

[3] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (Testo rilevante ai fini del SEE).

[4] Compresa la sentenza 6 ottobre 2015 nella causa C-362/14, Maximillian Schrems contro Data Protection Commissioner.

[5] Cfr. l'articolo 45, paragrafo 3, e l'articolo 93, paragrafo 2, del regolamento per ulteriori informazioni sugli atti di esecuzione.

[6] Sentenza 6 ottobre 2015 nella causa C-362/14, Maximillian Schrems contro Data Protection Commissioner (punti 73-74).

[7] Articolo 288, paragrafo 2, TFUE.

[8] Sentenza 6 ottobre 2015 nella causa C-362/14, Maximillian Schrems contro Data Protection Commissioner (punto 52).

[9] Considerando 105 del regolamento.

[10] Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) [Documento di lavoro 01/2016 sulla giustificazione delle ingerenze nei diritti fondamentali alla vita privata e alla protezione dei dati tramite misure di sorveglianza durante i trasferimenti di dati personali (Garanzie sostanziali europee)], 16/EN WP 237, 13 aprile 2016.

[11] Sentenza 6 ottobre 2015 nella causa C-362/14, Maximillian Schrems contro Data Protection Commissioner (punto 65).

[12] Tali categorie particolari sono dette anche "dati sensibili" al considerando 10 del regolamento.

[13] Sentenza 6 ottobre 2015 nella causa C-362/14, Maximillian Schrems contro Data Protection Commissioner (punto 74).

[14] Sentenza 6 ottobre 2015 nella causa C-362/14, Maximillian Schrems contro Data Protection Commissioner (punto 74).

Documento di lavoro che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa [WP 256 rev. 01]

Adottato il 28 novembre 2017
Versione emendata e adottata il 6 febbraio 2018

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'Unione europea per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della Commissione europea, direzione generale Giustizia e consumatori, B-1049 Bruxelles, Belgio, ufficio MO-59 05/035.

Sito Internet: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

INTRODUZIONE

Al fine di facilitare l'utilizzo delle norme vincolanti d'impresa per i titolari del trattamento (*Binding Corporate Rules for Controllers*,"BCR-C") da parte di un gruppo imprenditoriale o di un gruppo di imprese che svolgono un'attività economica comune per i trasferimenti internazionali da organismi stabiliti nell'Unione europea ("UE") a organismi dello stesso gruppo al di fuori dell'UE, il Gruppo di lavoro articolo 29 ("Gruppo") ha modificato il documento di lavoro 153 (adottato nel 2008) che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa ("BCR") per riflettere i requisiti relativi alle BCR ora espressamente definiti dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) ("regolamento")[1].

È opportuno ricordare che le BCR-C si applicano ai trasferimenti di dati personali da titolari del trattamento stabiliti nell'UE ad altri titolari del trattamento o responsabili del trattamento (stabiliti al di fuori dell'UE) dello stesso gruppo, mentre le norme vincolanti d'impresa per i responsabili del trattamento (*Binding Corporate Rules for Processors*, "BCR-P") si applicano ai dati ricevuti da un titolare del trattamento (stabilito nell'UE) non facente parte del gruppo e successivamente trattati dai membri del gruppo interessato in qualità di responsabili e/o sub-responsabili del trattamento. Pertanto, gli obblighi stabiliti nelle BCR-C valgono in relazione a soggetti dello stesso gruppo che fungono da titolari del trattamento e a soggetti che fungono da responsabili del trattamento "interni". Per quanto concerne quest'ultimo caso, occorre ricordare che con tutti i subcontraenti/responsabili del trattamento interni ed esterni si dovrebbe sottoscrivere un contratto o altro atto giuridico a norma del diritto dell'Unione o dello Stato membro, che vincoli il responsabile del trattamento al titolare del trattamento e che comprenda tutti i requisiti di cui all'articolo 28, paragrafo 3, del regolamento (per esempio, accordo di servizio o altro strumento che soddisfi gli stessi requisiti)[2]. Infatti, gli obblighi stabiliti nelle BCR-C si applicano ai soggetti del gruppo che ricevono i dati personali in qualità di responsabili del trattamento ("interni") nella misura in cui ciò non è in contrasto con l'accordo di servizio (vale a dire che i membri del gruppo responsabili del trattamento che effettuano il trattamento per conto dei membri del gruppo titolari del trattamento sono tenuti a rispettare in primo luogo tale contratto).

Tenuto conto del fatto che l'articolo 47, paragrafo 2, del regolamento stabilisce una serie minima di elementi da inserire nelle norme vincolanti d'impresa, la presente tabella modificata intende:

- adeguare la formulazione dei precedenti criteri di riferimento onde uniformarli all'articolo 47 del regolamento;

- chiarire il contenuto necessario delle BCR come stabilito all'articolo 47 (tenendo conto dei documenti WP74[3] e WP108[4] adottati dal Gruppo nel quadro della direttiva 95/46/CE);

- operare una distinzione tra ciò che deve essere incluso nelle BCR e ciò che deve essere presentato all'autorità di controllo competente nella domanda di BCR (documento WP133[5]);

- dotare i principi dei corrispondenti riferimenti testuali di cui all'articolo 47 del regolamento;

- fornire spiegazioni/osservazioni su ciascun principio.

L'articolo 47 del regolamento è chiaramente modellato sui documenti di lavoro relativi alle BCR adottati dal Gruppo. Tuttavia, esso specifica alcuni elementi nuovi di cui si deve tenere conto quando si aggiornano le BCR già esistenti o si adottano nuovi gruppi di BCR al fine di garantirne la compatibilità con il nuovo quadro stabilito dal regolamento.

1.1 ELEMENTI NUOVI

In tale ottica, il Gruppo intende richiamare l'attenzione in particolare sui seguenti elementi:

- ***diritto di proporre reclamo***: agli interessati dovrebbe essere concesso il diritto di proporre, a loro discrezione, reclamo a un'autorità di controllo nello Stato membro in cui risiedono abitualmente, lavorano oppure del luogo ove si è verificata la presunta violazione (ai sensi dell'articolo 77 del regolamento) oppure ricorso alle autorità giurisdizionali competenti degli Stati membri dell'UE (possibilità dell'interessato di promuovere un'azione dinanzi alle autorità giurisdizionali dello Stato membro in cui l'esportatore di dati ha uno stabilimento o l'interessato risiede abitualmente [articolo 79 del regolamento]);

- ***trasparenza***: a tutti gli interessati che godono dei diritti del terzo beneficiario si dovrebbero fornire, in particolare, le informazioni di cui agli articoli 13 e 14 del regolamento e le informazioni riguardanti i loro diritti in relazione al trattamento e i mezzi per esercitarli, la clausola in materia di responsabilità e le clausole relative ai principi di protezione dei dati;

- ***ambito di applicazione***: le BCR dovrebbero specificare la struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e di ciascuno dei suoi membri (articolo 47, paragrafo 2, lettera a), del regolamento), nonché il proprio ambito di applicazione materiale, ad esempio i trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione (articolo 47, paragrafo 2, lettera b), del regolamento);

- ***principi di protezione dei dati***: unitamente ai principi di trasparenza, correttezza, limitazione della finalità, qualità dei dati e sicurezza, le BCR dovrebbero anche spiegare gli altri principi di cui all'articolo 47, paragrafo 2, lettera d), quali, in particolare, i principi di liceità, minimizzazione dei dati, limitazione del periodo di conservazione, garanzie nel trattamento di categorie particolari di dati personali, e i requisiti per i trasferimenti successivi ad organismi che non sono vincolati dalle norme vincolanti d'impresa;

- ***responsabilizzazione***: ogni soggetto che agisce in qualità di titolare del trattamento è competente per il rispetto delle BCR e in grado di comprovarlo (articolo 5, paragrafo 2, del regolamento);

- ***legislazione del paese terzo***: le BCR dovrebbero prevedere un impegno secondo cui, qualora un requisito di legge cui è soggetto un membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune in un paese terzo possa avere effetti negativi sostanziali sulle garanzie fornite dalle BCR, il problema sia segnalato all'autorità di controllo competente (salvo che ciò sia vietato da norme specifiche, ad esempio da norme di diritto penale a tutela del segreto delle indagini). Ciò include qualsiasi richiesta giuridicamente vincolante di comunicazione di dati personali presentata da un'autorità giudiziaria o da un servizio di sicurezza nazionale.

1.2 MODIFICHE DI BCR GIÀ ADOTTATE

Sebbene, conformemente all'articolo 46, paragrafo 5, del regolamento, le autorizzazioni rilasciate da uno Stato membro o dall'autorità di controllo in base all'articolo 26, paragrafo 2, della direttiva 95/46/CE restino valide fino a quando non vengono modificate, sostituite o abrogate, se necessario, dalla medesima autorità di controllo, i gruppi che hanno BCR approvate dovrebbero, nel prepararsi all'applicazione del regolamento, allineare le loro BCR ai requisiti del regolamento.

Il presente documento mira ad aiutare i gruppi con BCR approvate ad attuare le modifiche pertinenti per allineare le BCR al regolamento. A tal fine, questi gruppi sono invitati a segnalare le modifiche pertinenti nell'ambito dell'obbligo (di cui al punto 5.1 del WP153) a tutti i membri del gruppo e alle autorità di protezione dei dati tramite l'autorità di protezione dei dati capofila nel quadro dell'aggiornamento annuo a partire dal 25 maggio 2018. Le BCR aggiornate possono essere utilizzate senza dover richiedere una nuova autorizzazione o approvazione.

Tenuto conto di quanto precede, le autorità di protezione dei dati si riservano il diritto di esercitare i loro poteri di cui all'articolo 46, paragrafo 5, del regolamento.

GRUPPO DI LAVORO
ARTICOLO 29
PER LA PROTEZIONE DEI DATI

Criteri di approvazione delle BCR	Nelle BCR	Nel modulo di domanda	Testi di riferimento	Osservazioni	Riferimenti alla domanda/ alle BCR[6]
1 - NATURA VINCOLANTE					
A LIVELLO INTERNO					
1.1 Obbligo di rispettare le BCR	SI	SI	Articolo 47, paragrafo 1, lettera a), e articolo 47, paragrafo 2, lettera c), del regolamento	Le BCR devono essere giuridicamente vincolanti e prevedere l'obbligo chiaro per ciascun membro partecipante del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune ("membro vincolato dalle BCR"), compresi i loro dipendenti, di rispettare le BCR.	
1.2 Spiegazione di come le norme sono rese vincolanti per i membri del gruppo vincolati dalle BCR e per i loro dipendenti	NO	SI	Articolo 47, paragrafo 1, lettera a), e articolo 47, paragrafo 2, lettera c), del regolamento	Il gruppo dovrà spiegare nel modulo di domanda in che modo le norme sono rese vincolanti: I) per ciascuna società partecipante/ ciascun soggetto del gruppo, mediante una o più delle opzioni seguenti: • contratto infragruppo; • accordi	

				unilaterali (ciò è possibile solo se il membro vincolato dalle BCR che ha la responsabilità si trova in uno Stato membro che riconosce gli accordi unilaterali come vincolanti e se tale membro è giuridicamente in grado di vincolare gli altri membri vincolati dalle BCR); • altri mezzi (solo se il gruppo dimostra il modo in cui viene conseguito il carattere vincolante delle BCR); II) per i dipendenti, mediante una o più delle seguenti opzioni: • contratto/ accordo individuale e distinto che prevede sanzioni; • clausola nel contratto di lavoro con una descrizione delle sanzioni applicabili; • politiche interne che prevedono sanzioni, o • contratti collettivi che	

				prevedono sanzioni; • altri mezzi (ma il gruppo deve spiegare in maniera adeguata come le BCR sono rese vincolanti per i dipendenti).	
A LIVELLO ESTERNO					
1.3 Creazione di diritti del terzo beneficiario per gli interessati, inclusa la possibilità di proporre reclamo all'autorità di controllo competente e di proporre ricorso alle autorità giurisdi-zionali	SI	SI	Articolo 47, paragrafo 1, lettera b), e articolo 47, paragrafo 2, lettere c) ed e), del regolamento	Le BCR devono conferire espressamente agli interessati diritti per far valere le BCR in qualità di terzi beneficiari. Gli interessati devono perlomeno essere in grado di far valere i seguenti elementi delle BCR: • principi di protezione dei dati (articolo 47, paragrafo 2, lettera d), e sezione 6.1 dei presenti criteri di riferimento); • trasparenza e facile accesso alle BCR (articolo 47, paragrafo 2, lettera g), e sezioni 6.1 e 1.7 dei presenti criteri di riferimento); • diritti di accesso, rettifica, cancellazione, limitazione, opposizione al trattamento, diritto di non essere sottoposti a decisioni che siano basate unicamente	

				su un trattamento automatizzato, inclusa la profilazione (articolo 47, paragrafo 2, lettera e), e articoli 15, 16, 17, 18, 21 e 22 del regolamento); • legislazione nazionale che impedisce il rispetto delle BCR (articolo 47, paragrafo 2, lettera m), e sezione 6.3 dei presenti criteri di riferimento); • diritto di proporre reclamo attraverso il meccanismo interno di reclamo delle imprese (articolo 47, paragrafo 2, lettera i), e sezione 2.2 dei presenti criteri di riferimento); • obblighi di cooperazione con le autorità di controllo (articolo 47, paragrafo 2, lettere k) e l), e sezione 3.1 dei presenti criteri di riferimento); • norme di responsabilità e giurisdizione (articolo 47, paragrafo 2, lettere e) e f), e sezioni 1.3 e 1.4 dei presenti criteri di riferimento). In particolare, le BCR	

				devono conferire il diritto di proporre reclamo all'autorità di controllo competente (scelta tra l'autorità di controllo dello Stato membro in cui si risiede abitualmente, si lavora oppure del luogo ove si è verificata la presunta violazione, ai sensi dell'articolo 77 del regolamento) e di proporre ricorso all'autorità giurisdizionale degli Stati membri dell'UE (possibilità per l'interessato di promuovere un'azione dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha sede o l'interessato risiede abitualmente, ai sensi dell'articolo 79 del regolamento). Le BCR dovrebbero espressamente conferire agli interessati il diritto a un ricorso giurisdizionale e il	

				diritto di ottenere riparazione e, se del caso, il risarcimento per violazione di uno degli elementi azionabili delle BCR elencati sopra (articoli da 77 a 82 del regolamento). Le imprese dovrebbero garantire che tutti questi diritti siano inclusi nella clausola del terzo beneficiario delle loro BCR, ad esempio facendo riferimento alle clausole/sezioni/ parti delle BCR in cui tali diritti sono disciplinati o elencandoli tutti nella clausola del terzo beneficiario. Tali diritti non si estendono a quegli elementi delle BCR che riguardano i meccanismi interni degli organismi, quali dettagli della formazione, programmi di revisione, rete di conformità e meccanismo di aggiornamento delle norme.	

1.4 La sede principale nell'Unione europea, il membro stabilito nell'UE con responsabilità delegate di protezione dei dati o l'esportatore di dati accetta di assumersi la responsabilità di pagare il risarcimento e di porre rimedio alle violazioni delle BCR	SI	SI	Articolo 47, paragrafo 2, lettera f), del regolamento	Le BCR devono includere l'obbligo per le sedi principali nell'UE o per un membro vincolato dalle BCR stabilito nell'UE con responsabilità delegate di accettare di assumersi la responsabilità e di concordare di intraprendere le azioni necessarie per porre rimedio agli atti di altri membri vincolati dalle BCR stabiliti al di fuori dell'UE nonché di pagare un risarcimento per gli eventuali danni materiali e immateriali causati dalla violazione delle BCR da parte di membri vincolati dalle BCR. Le BCR devono inoltre stabilire che, se un membro vincolato dalle BCR stabilito al di fuori dell'UE viola le BCR, le autorità giurisdizionali o altre autorità competenti dell'UE avranno la giurisdizione e che l'interessato disporrà dei diritti e dei mezzi di ricorso nei confronti del membro vincolato dalle BCR che ha accettato di di assumersi la	

				responsabilità come se la violazione fosse stata causata da lui stesso nello Stato membro in cui ha sede anziché dal membro vincolato dalle BCR stabilito al di fuori dell'UE. Un'altra opzione, specialmente se per un gruppo con strutture societarie particolari non è possibile imporre a un soggetto specifico di assumersi l'intera responsabilità per qualsiasi violazione delle BCR al di fuori dell'UE, può prevedere che ogni membro vincolato dalle BCR che esporta dati al di fuori dell'UE sulla base delle BCR sia responsabile delle violazioni delle BCR da parte del membro vincolato dalle BCR stabilito al di fuori dell'UE che ha ricevuto i dati da tale membro vincolato dalle BCR stabilito nell'UE.	
1.5 L'impresa dispone di risorse sufficienti	NO	SI	[WP 74, punto 5.5.2., paragrafo 2 (pagina 18) + WP108 punto 5.17. (pagina 6)]	Il modulo di domanda deve contenere la conferma che il membro vincolato dalle BCR che ha accettato di assumersi la responsabilità degli atti di altri membri	

				vincolati alle BCR stabiliti al di fuori dell'UE dispone di risorse sufficienti per corrispondere i risarcimenti dei danni risultanti dalle violazioni delle BCR.	
1.6 L'onere della prova spetta all'impresa, non al singolo	SI	SI	Articolo 47, paragrafo 2, lettera f), del regolamento	Le BCR devono stabilire che al membro vincolato dalle BCR che ha accettato di assumersi la responsabilità spetti l'onere di dimostrare che il membro vincolato dalle BCR stabilito al di fuori dell'UE non è responsabile della violazione delle norme per la quale l'interessato chiede il risarcimento del danno. Se il membro vincolato dalle BCR che ha accettato di assumersi la responsabilità è in grado di dimostrare che il membro vincolato dalle BCR stabilito al di fuori dell'UE non è responsabile dell'evento che ha determinato il danno, può ritenersi sollevato da qualunque responsabilità.	

1.7 Trasparenza e facile accesso alle BR per gli interessati	SI	NO	Articolo 47, paragrafo 2, lettera g), del regolamento	Le BCR devono contenere l'impegno secondo cui a tutti gli interessati che godono dei diritti del terzo beneficiario si dovrebbero fornire le informazioni previste agli articoli 13 e 14 del regolamento, le informazioni riguardanti i loro diritti del terzo beneficiario relativi al trattamento dei dati personali che li riguardano e i mezzi per esercitare tali diritti, la clausola in materia di responsabilità e le clausole riguardanti i principi di protezione dei dati. Le informazioni devono essere fornite in maniera completa; una sintesi non sarà sufficiente. Le BCR devono contenere il diritto di ogni interessato di avere facile accesso alle stesse. Ad esempio, le BCR potrebbero stabilire che come minimo le parti delle BCR per le quali è obbligatorio fornire informazioni agli interessati (come descritto al paragrafo	

				precedente) siano pubblicate su Internet o sull'Intranet (nel caso in cui gli interessati siano solo membri del personale dell'impresa che hanno accesso all'Intranet).	
2 - EFFICACIA					
2.1 Esistenza di un programma di formazione appropriato	SI	SI	Articolo 47, paragrafo 2, lettera n), del regolamento	Le BCR devono stabilire che sarà fornita una formazione appropriata sulle BCR al personale che ha accesso permanente o regolare ai dati personali, che è coinvolto nella raccolta dei dati o nello sviluppo di strumenti utilizzati per il trattamento dei dati personali. Le autorità di controllo che valutano le BCR potranno richiedere esempi e spiegazioni del programma di formazione nel corso della procedura di domanda. Il programma di formazione dovrebbe essere specificato nella domanda.	

2.2 Esistenza di un processo di gestione dei reclami per le BCR	SI	SI	Articolo 47, paragrafo 2, lettera i), e articolo 12, paragrafo 3, del regolamento	Le BCR devono istituire un processo interno di gestione dei reclami per garantire che qualsiasi interessato sia in grado di esercitare i propri diritti e proporre reclamo nei confronti di qualsiasi membro vincolato dalle BCR. • I reclami devono essere gestiti senza ingiustificato ritardo, in ogni caso entro un mese, da parte di un reparto o una persona chiaramente identificati che abbia un livello adeguato di indipendenza nell'esercizio delle proprie funzioni. Tenuto conto della complessità e del numero di domande, detto periodo di un mese può essere prorogato al massimo di altri due mesi, nel qual caso l'interessato dovrà esserne informato di conseguenza. Il modulo di domanda deve spiegare il modo in cui gli interessati saranno informati delle fasi pratiche del sistema di reclamo, in particolare:	

				• l'organo a cui proporre reclamo; • la forma in cui i reclami devono essere presentati; • i tempi per la risposta a un reclamo; • le conseguenze in caso di rigetto del reclamo; • le conseguenze nel caso in cui il reclamo sia considerato giustificato; • le conseguenze nel caso in cui l'interessato non sia soddisfatto delle risposte (diritto di proporre ricorso all'autorità giurisdizionale e reclamo all'autorità di controllo).	
2.3 Esistenza di un programma di verifica esteso alle BCR	SI	SI	Articolo 47, paragrafo 2, lettere j) e l), e articolo 38, paragrafo 3, del regolamento	Le BCR devono istituire l'obbligo per il gruppo di prevedere verifiche sulla protezione dei dati su base periodica (da parte di revisori accreditati interni o esterni) o su richiesta specifica del responsabile/ dell'ufficio competente per la tutela della vita privata (o di qualsiasi altra carica competente all'interno dell'organizzazione)	

				al fine di garantire la verifica della conformità alle BCR. Le BCR devono stabilire che il programma di verifica riguardi tutti gli aspetti delle BCR, inclusi i metodi per assicurare provvedimenti correttivi. Devono inoltre stabilire che il risultato sia comunicato al responsabile/ all'ufficio per la tutela della vita privata e al consiglio di amministrazione competente della società controllante di un gruppo o del gruppo di imprese che svolgono un'attività economica comune. Se del caso, il risultato potrà essere comunicato al consiglio di amministrazione della società madre. Le BCR devono stabilire che le autorità di controllo possono avere accesso, su richiesta, ai risultati delle verifiche, e devono conferire loro l'autorità/la facoltà di effettuare esse stesse una verifica sulla protezione dei dati di qualsiasi	

				membro vincolato dalle BCR, se necessario. Il modulo di domanda conterrà una descrizione del sistema di verifica. Ad esempio: • il soggetto (reparto all'interno del gruppo) che decide il piano/ programma di verifica; • il soggetto che conduce l'attività di verifica; • la frequenza dell'attività di verifica (periodica o su richiesta specifica dell'ufficio competente in materia di tutela della vita privata); • ambito della verifica (ad esempio, applicazioni, sistemi informatici, banche dati che trattano dati personali o trasferimenti successivi, decisioni adottate riguardo alle disposizioni vincolanti della legislazione nazionale che sono in contrasto con le BCR, la verifica delle clausole contrattuali per i trasferimenti fuori	

				dal gruppo (verso titolari del trattamento o responsabili del trattamento), provvedimenti correttivi, ecc.); • il soggetto che riceve i risultati delle attività di verifica.	
2.4 Creazione di una rete di responsabili della protezione dei dati o personale adeguato preposto al monito-raggio della conformità alle norme	SI	NO	Articolo 47, paragrafo 2, lettera h), e articolo 38, paragrafo 3, del regolamento	Le BCR dovrebbero prevedere un impegno a designare un responsabile della protezione dei dati, ove richiesto, in linea con l'articolo 37 del regolamento, o una qualsiasi altra persona o soggetto (quale un responsabile della vita privata) avente la responsabilità di monitorare la conformità alle BCR che goda del massimo supporto gestionale per l'adempimento di tale compito. Il responsabile della protezione dei dati o altro professionista della vita privata può essere assistito da una squadra, una rete di responsabili della protezione dei dati o contatti locali, a seconda del caso. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico	

				(articolo 38, paragrafo 3, del regolamento). Le BCR dovrebbero includere una breve descrizione della struttura interna, del ruolo, della posizione e dei compiti del responsabile della protezione dei dati o di una carica analoga e della rete creata per garantire la conformità alle norme. Ad esempio, dovrebbero indicare che il responsabile della protezione dei dati o il responsabile della vita privata fornisce informazioni e consulenza al vertice gerarchico, si occupa delle indagini delle autorità di controllo, monitora e riferisce annualmente sulla conformità a livello globale, e che i responsabili della protezione o i contatti locali possono essere incaricati di gestire i reclami locali degli interessati, riferire sulle questioni di maggiore rilevanza in materia di vita privata al responsabile della protezione dei dati e monitorare la formazione e la conformità a livello locale.	

3 - OBBLIGO DI COOPERAZIONE					
3.1 Obbligo di cooperazione con le autorità di controllo	SI	SI	Articolo 47, paragrafo 2, lettera l), del regolamento	Le BCR dovrebbero includere l'obbligo chiaro per tutti i membri vincolati dalle BCR di cooperare con le autorità di controllo, di accettare di essere controllati dalle stesse e di conformarsi a quanto raccomandato da tali autorità riguardo a qualsiasi aspetto connesso alle norme.	
4 - DESCRIZIONE DEL TRATTAMENTO E DEI FLUSSI DI DATI					
4.1 Descrizione dell'ambito di applicazione materiale delle BCR (natura dei dati trasferiti, tipo di interessati, paesi)	SI	SI	Articolo 47, paragrafo 2, lettera b), del regolamento	Le BCR devono specificare il loro ambito di applicazione materiale e pertanto contenere una descrizione generale dei trasferimenti al fine di consentire alle autorità di controllo di valutare la conformità del trattamento svolto nei paesi terzi. Le BCR devono in particolare specificare i trasferimenti o il complesso di trasferimenti di dati, inclusi la natura e le categorie di dati personali, il tipo di trattamento e le relative finalità, il tipo di interessati (dati relativi a	

				dipendenti, clienti, fornitori e altri terzi nell'ambito delle loro rispettive attività commerciali regolari) e l'identificazione del paese terzo o dei paesi terzi in questione.	
4.2 Indicazione dell'ambito geografico delle BCR	SI	SI	Articolo 47, p aragrafo 2, lettera a), del regolamento	Le BCR dovrebbero specificare la struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e di ciascuno dei suoi membri. Le BCR dovrebbero indicare se si applicano a: I) tutti i dati personali trasferiti dall'Unione europea all'interno del gruppo, OPPURE II) tutti i trattamenti di dati personali all'interno del gruppo.	
5 - MECCANISMI PER RIFERIRE E REGISTRARE LE MODIFICHE					
5.1 Processo per l'aggiornamento delle BCR	SI	SI	Articolo 47, paragrafo 2, lettera k), del regolamento	Le BCR possono essere modificate (*ad esempio, per tenere conto di modifiche del contesto normativo o della struttura societaria*)	

				ma dovrebbero imporre l'obbligo di segnalare le modifiche senza ingiustificato ritardo, tramite l'autorità di controllo competente, a tutti i membri vincolati dalle BCR e alle autorità di controllo interessate. Le BCR e l'elenco dei membri vincolati dalle BCR possono essere aggiornati senza che sia necessario presentare una nuova domanda di approvazione a condizione che: I) una persona o una squadra/reparto identificati tenga un elenco completamente aggiornato dei membri vincolati dalle BCR e conservi registrazioni degli aggiornamenti delle norme e fornisca le informazioni necessarie agli interessati o, su richiesta, alle autorità di controllo; II) non sia effettuato alcun trasferimento a un nuovo membro	

				vincolato dalle BCR finché quest'ultimo non sia effettivamente vincolato dalle BCR e possa garantirne il rispetto; III) le eventuali modifiche delle BCR o dell'elenco dei membri vincolati dalle BCR siano comunicate una volta all'anno alle autorità di controllo interessate tramite l'autorità di controllo competente, con una breve spiegazione dei motivi che giustificano l'aggiornamento; IV) sia comunicata prontamente alle autorità di controllo interessate, tramite l'autorità di controllo competente, qualsiasi modifica che possa compromettere il livello di protezione offerto dalle BCR o incidere significativa-mente sulle BCR (per esempio, modifiche del carattere vincolante).	

6 - GARANZIE DI PROTEZIONE DEI DATI					
6.1.1 Descrizione dei principi di protezione dei dati, incluse le norme sui trasferimenti o trasferimenti successivi al di fuori dell'UE	SI	SI	Articolo 47, paragrafo 2, lettera d), del regolamento	Le BCR dovrebbero includere esplicitamente i seguenti principi che devono essere osservati dalle imprese: I) trasparenza, correttezza e liceità (articolo 5, paragrafo 1, lettera a), e articoli 6, 9, 10, 13 e 14 del regolamento); II) limitazione della finalità (articolo 5, paragrafo 1, lettera b), del regolamento); III) minimizzazione dei dati ed esattezza (articolo 5, paragrafo 1, lettere c) e d), del regolamento); IV) periodi di conservazione limitati (articolo 5, paragrafo 1, lettera e), del regolamento); V) trattamento di categorie particolari di dati personali; VI) sicurezza (articolo 5, lettera f), e articolo 32 del regolamento), incluso l'obbligo di stipulare contratti con tutti i sub-contraenti/	

				responsabili del trattamento interni ed esterni, che comprendano tutti i requisiti di cui all'articolo 28, paragrafo 3, del regolamento nonché l'obbligo di segnalare senza ingiustificato ritardo eventuali violazioni di dati personali alle sedi principali nell'UE o al membro vincolato dalle BCR stabilito nell'UE con responsabilità delegate di protezione dei dati, all'altro responsabile/ ufficio per la tutela della vita privata e, se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, agli interessati. Inoltre, le violazioni di dati personali dovrebbero essere documentate (comprese le circostanze relative alla violazione, le conseguenze e i	

				provvedimenti adottati per porvi rimedio) e la documentazione dovrebbe essere messa a disposizione dell'autorità di controllo, su richiesta (articoli 33 e 34 del regolamento); VII) limitazioni ai trasferimenti e ai trasferimenti successivi a responsabili del trattamento e titolari del trattamento non facenti parte del gruppo (i membri vincolati dalle BCR che sono titolari del trattamento possono trasferire dati ai responsabili del trattamento/ titolari del trattamento al di fuori del gruppo stabiliti al di fuori dell'UE, purché sia garantito un livello adeguato di protezione ai sensi degli articoli 45, 46, 47 e 48 del regolamento o trovi	

				applicazione una deroga di cui all'articolo 49 del regolamento). La formulazione e le definizioni dei principi chiave delle BCR dovrebbero essere coerenti con quelle del regolamento.	
6.1.2 Responsabilizzazione e altri strumenti	SI	SI	Articolo 47, paragrafo 2, lettera d), e articolo 30 del regolamento	Ogni soggetto che agisce in qualità di titolare del trattamento è competente per il rispetto delle BCR e in grado di comprovarlo (articolo 5, paragrafo 2, e articolo 24 del regolamento). Al fine di dimostrare la conformità, i membri vincolati dalle BCR devono tenere un registro di tutte le categorie di attività di trattamento svolte in linea con i requisiti stabiliti all'articolo 30, paragrafo 1, del regolamento. Tale registro dovrebbe essere tenuto in forma scritta, anche in formato elettronico, e, su richiesta, essere messo a disposizione dell'autorità di controllo. Al fine di migliorare la conformità e	

				quando richiesto, dovrebbero essere effettuate valutazioni d'impatto sulla protezione dei dati per le attività di trattamento che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche (articolo 35 del regolamento). Qualora una valutazione d'impatto sulla protezione dei dati di cui all'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio, prima del trattamento dovrebbe essere consultata l'autorità di controllo competente (articolo 36 del regolamento). Dovrebbero essere messe in atto misure tecniche e organizzative adeguate volte ad attuare i principi di protezione dei dati e a facilitare la conformità ai requisiti stabiliti dalle BCR nella	

				prassi (protezione dei dati fin dalla progettazione e protezione per impostazione definita, articolo 25 del regolamento).	
6.2 Elenco dei soggetti vincolati dalle BCR	SI	SI	Articolo 47, paragrafo 2, lettera a), del regolamento	Le BCR devono contenere un elenco dei soggetti vincolati dalle BCR, incluse le coordinate di contatto.	
6.3 Necessità di trasparenza nei casi in cui la legislazione nazionale impedisca al gruppo di conformarsi alle BCR	SI	NO	Articolo 47, paragrafo 2, lettera m), del regolamento	Le BCR dovrebbero prevedere un impegno chiaro secondo cui, qualora un membro vincolato dalle BCR abbia motivo di ritenere che la legislazione applicabile impedisca all'impresa di ottemperare agli obblighi derivanti dalle BCR o abbia effetti negativi sostanziali sulle garanzie fornite dalle BCR, lo comunichi tempestivamente alla sede principale nell'UE o al membro vincolato dalle BCR stabilito nell'UE con responsabilità delegate di protezione dei dati e all'altro responsabile/ufficio competente per la protezione della vita privata (fatti salvi i divieti di un'autorità	

				giudiziaria, ad esempio il divieto imposto da norme di diritto penale a tutela del segreto delle indagini). Le BCR dovrebbero prevedere inoltre un impegno secondo cui, qualora un requisito di legge cui è soggetto un membro vincolato dalle BCR in un paese terzo possa avere effetti negativi sostanziali sulle garanzie fornite dalle BCR, il problema sia segnalato all'autorità di controllo competente. Ciò include qualsiasi richiesta giuridicamente vincolante di comunicazione di dati personali presentata da un'autorità giudiziaria o da un servizio di sicurezza nazionale. In tal caso, l'autorità di controllo competente dovrebbe essere chiaramente informata della richiesta, comprese le informazioni sui dati richiesti, sull'organo richiedente e sulla base giuridica della	

				comunicazione (salvo che ciò sia vietato da norme specifiche, ad esempio da norme di diritto penale a tutela del segreto delle indagini). Se, in casi specifici, la sospensione e/o la segnalazione sono vietate, le BCR devono prevedere che il membro vincolato dalle BCR si adoperi per ottenere il diritto di rinuncia al divieto al fine di comunicare quanto prima la maggiore quantità di informazioni, e sia in grado di dimostrare di aver agito in tal senso. Se, nei casi di cui sopra, nonostante tutti gli sforzi, il membro vincolato dalle BCR non si trovi nella posizione di poter informare l'autorità di controllo competente, esso deve impegnarsi nelle BCR a fornire annualmente all'autorità di controllo competente informazioni generali sulle richieste ricevute (per esempio, numero di richieste di comunicazione, tipo di dati richiesti,	

				richiedente se possibile, ecc.). In ogni caso, le BCR devono stabilire che i trasferimenti di dati personali da un membro del gruppo vincolato dalle BCR all'autorità pubblica non possono essere massicci, sproporzionati e indiscriminati da andare oltre quanto necessario in una società democratica.	
6.4 Specificazione del rapporto tra il diritto nazionale e le BCR	SI	NO	N.D.	Le BCR devono specificare il loro rapporto con il diritto applicabile in materia. Le BCR devono stabilire che, qualora il diritto locale, ad esempio quello dell'UE, richieda un livello di protezione dei dati personali più elevato, tale diritto prevalga sulle BCR. I dati personali saranno trattati in ogni caso secondo il diritto applicabile come previsto dall'articolo 5 del regolamento e dal diritto locale in materia.	

NOTE

[1] Testo rilevante ai fini del SEE.

[2] L'articolo 28, paragrafo 3, impone, tra le altre cose, per ciascun rapporto tra titolare del trattamento e responsabile del trattamento, un'indicazione precisa, mediante contratto o altro atto giuridico, della materia disciplinata, della durata, della natura e delle finalità del trattamento, del tipo di dati personali e delle categorie di interessati, nonché degli obblighi e dei diritti del titolare del trattamento. L'inclusione nelle BCR di una descrizione generica delle categorie di dati, degli interessati, ecc. non sarebbe sufficiente a tale riguardo.

[3] Documento di lavoro WP74: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers (Trasferimenti di dati personali a paesi terzi: applicazione dell'articolo 26, paragrafo 2, della direttiva dell'UE sulla protezione dei dati alle norme vincolanti d'impresa per i trasferimenti internazionali di dati), adottato il 3 giugno 2003, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf.

[4] Documento di lavoro WP108: Establishing a model checklist application for approval of Binding Corporate Rules (Definizione di un modello di checklist per l'approvazione delle norme vincolanti d'impresa), adottato il 14 aprile 2005, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp108_en.pdf.

[5] Documento di lavoro WP133: Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data (Raccomandazione 1/2007 sulla domanda standard per l'approvazione delle norme vincolanti d'impresa per il trasferimento di dati personali), adottato il 10 gennaio 2007, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp133_en.doc.

[6] Da completare a cura del richiedente.

Documento di lavoro che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa per i responsabili del trattamento [WP 257 rev. 01]

Adottato il 28 novembre 2017
Versione emendata e adottata il 6 febbraio 2018

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'Unione europea per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della Commissione europea, direzione generale Giustizia e consumatori, B-1049 Bruxelles, Belgio, ufficio MO-59 02/013.

Sito Internet: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

INTRODUZIONE

Al fine di facilitare l'utilizzo delle norme vincolanti d'impresa per i responsabili del trattamento (*Binding Corporate Rules for Processors*, "BCR-P") da parte di un gruppo imprenditoriale o di un gruppo di imprese che svolgono un'attività economica comune per i trasferimenti internazionali da organismi stabiliti nell'Unione europea ("UE") a organismi dello stesso gruppo al di fuori dell'UE, il Gruppo di lavoro articolo 29 ("Gruppo") ha modificato il documento di lavoro 195 (adottato nel 2012) che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa ("BCR") per riflettere i requisiti relativi alle BCR ora espressamente definiti dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) ("regolamento").

È opportuno ricordare che le BCR-P si applicano ai dati ricevuti da un titolare del trattamento stabilito nell'UE non facente parte del gruppo e successivamente trattati dai membri del gruppo in qualità di responsabili e/o sub-responsabili del trattamento, mentre le norme vincolanti d'impresa per i titolari del trattamento (*BCRs for Controllers*, "BCR-C") si applicano ai trasferimenti di dati personali da titolari del trattamento stabiliti nell'UE ad altri titolari del trattamento o a responsabili del trattamento dello stesso gruppo stabiliti al di fuori dell'UE. Pertanto, gli obblighi stabiliti nelle BCR-P valgono in relazione ai dati personali di terzi trattati da un membro del gruppo in qualità di responsabile del trattamento secondo le istruzioni di un titolare del trattamento non appartenente al gruppo.

Conformemente all'articolo 28, paragrafo 3, del regolamento, il titolare e il responsabile del trattamento devono stipulare un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento. Tale contratto o un altro atto giuridico verrà definito in questa sede "accordo di servizio".

Tenuto conto del fatto che l'articolo 47, paragrafo 2, del regolamento stabilisce che le norme vincolanti d'impresa devono contenere una serie minima di elementi, la presente tabella modificata intende:

- adeguare la formulazione dei precedenti criteri di riferimento onde uniformarli all'articolo 47 del regolamento;
- chiarire il contenuto necessario di una BCR come stabilito all'articolo 47 e nel documento WP204[1] adottato dal Gruppo nel quadro della direttiva 95/46/CE);
- operare una distinzione tra ciò che deve essere incluso nelle BCR e ciò che deve essere presentato all'autorità di controllo competente nella domanda di BCR (documento WP 195a[2]), e
- fornire spiegazioni/osservazioni su ogni requisito.

L'articolo 47 del regolamento è chiaramente modellato sui documenti di lavoro relativi alle BCR adottati dal Gruppo. Tuttavia, esso specifica alcuni elementi nuovi di cui si deve tenere conto quando si aggiornano le BCR approvate già esistenti o si adottano nuovi gruppi di BCR al fine di garantirne la compatibilità con il nuovo quadro stabilito dal regolamento.

1. NUOVI ELEMENTI

In tale ottica, il Gruppo intende richiamare l'attenzione in particolare sui seguenti elementi:

- ***ambito di applicazione***: le BCR dovrebbero specificare la struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese che svolge un'attività economica comune e di ciascuno dei suoi membri (articolo 47, paragrafo 2, lettera a), del regolamento), nonché il proprio ambito di applicazione materiale, ad esempio i trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione (articolo 47, paragrafo 2, lettera b), del regolamento);
- ***diritti del terzo beneficiario***: gli interessati dovrebbero essere in grado di far valere le BCR in qualità di terzi beneficiari direttamente nei confronti del responsabile del trattamento qualora le disposizioni in questione siano specificatamente dirette ai responsabili del trattamento, conformemente al regolamento (articoli 28, 29, 79);
- ***diritto di proporre reclamo***: agli interessati dovrebbe essere concesso il diritto di proporre, a loro discrezione, reclamo a un'autorità di controllo nello Stato membro in cui risiedono abitualmente, lavorano oppure del luogo ove si è verificata la presunta violazione (ai sensi dell'articolo 77 del regolamento) oppure ricorso alle autorità giurisdizionali competenti degli Stati membri dell'UE (possibilità dell'interessato di promuovere un'azione dinanzi alle autorità giurisdizionali dello Stato membro in cui l'esportatore di dati ha uno stabilimento o l'interessato risiede abitualmente [articolo 79 del regolamento]);
- ***principi di protezione dei dati***: unitamente agli obblighi derivanti da principi di trasparenza, correttezza, liceità, limitazione della finalità, qualità dei dati e sicurezza, le BCR dovrebbero inoltre spiegare in che modo il responsabile del trattamento osserverà altri requisiti, come, in particolare, quelli relativi ai diritti degli interessati, ai subcontratto e ai trasferimenti successivi a soggetti non vincolati dalle BCR;
- ***responsabilizzazione***: i responsabili del trattamento avranno l'obbligo di mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi tramite, tra l'altro, attività di revisione e ispezioni realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato (articolo 28, paragrafo 3, lettera h), del regolamento);

- ***accordo di servizio***: l'accordo di servizio tra il titolare e il responsabile del trattamento deve contenere tutti gli elementi necessari previsti dall'articolo 28 del regolamento.

2. MODIFICHE DI BCR GIÀ ADOTTATE

Sebbene, conformemente all'articolo 46, paragrafo 5, del regolamento, le autorizzazioni rilasciate da uno Stato membro o dall'autorità di controllo in base all'articolo 26, paragrafo 2, della direttiva 95/46/CE restino valide fino a quando non vengono modificate, sostituite o abrogate, se necessario, dalla medesima autorità di controllo, i gruppi che hanno BCR approvate dovrebbero, nel prepararsi all'applicazione del regolamento, allineare le loro BCR ai requisiti del regolamento.

Il presente documento mira ad aiutare i gruppi con BCR approvate ad attuare le modifiche pertinenti per allineare le BCR al regolamento. A tal fine, questi gruppi sono invitati a segnalare le modifiche pertinenti nell'ambito dell'obbligo (di cui al punto 5.1 del WP195) a tutti i membri del gruppo e alle autorità di protezione dei dati tramite l'autorità di protezione dei dati capofila nel quadro dell'aggiornamento annuo a partire dal 25 maggio 2018. Le BCR aggiornate possono essere utilizzate senza dover richiedere una nuova autorizzazione o approvazione da parte delle autorità competenti per la protezione dei dati personali.

Tenuto conto di quanto precede, le autorità di protezione dei dati si riservano il diritto di esercitare i loro poteri di cui all'articolo 46, paragrafo 5, del regolamento.

Criteri di approvazione delle BCR	Nelle BCR	Nel modulo di domanda	Osservazioni	Riferimenti alla domanda/ alle BCR
1 - NATURA VINCOLANTE				
A LIVELLO INTERNO				
1.1 Obbligo di rispettare le BCR	SI	SI	Le BCR devono essere giuridicamente vincolanti e prevedere l'obbligo chiaro per ciascun membro partecipante del gruppo imprenditoriale o del gruppo di imprese che svolge un'attività economica comune ("membro vincolato dalle BCR"), compresi i loro dipendenti, di rispettare le BCR. Le BCR devono inoltre stabilire esplicitamente che ogni membro, compresi i dipendenti, deve rispettare le istruzioni del responsabile del trattamento riguardanti il trattamento dei dati e le misure di sicurezza e di riservatezza conformemente all'accordo di servizio (articoli 28, 29 e 32 del regolamento).	
1.2 Spiegazione di come le norme sono rese vincolanti per i membri del gruppo e per i loro dipendenti	NO	SI	Il gruppo dovrà spiegare nel modulo di domanda in che modo le norme sono rese vincolanti: I) per ogni membro vincolato dalle BCR, mediante una o più delle seguenti opzioni: • contratto infragruppo; • accordi unilaterali (ciò è possibile solo se il membro vincolato dalle BCR che ha la responsabilità si trova in uno Stato membro che riconosce gli accordi unilaterali come vincolanti e se tale membro è giuridicamente in grado di vincolare gli altri membri vincolati dalle BCR), o • altri mezzi (solo se il gruppo dimostra il modo in cui viene conseguito il carattere vincolante delle BCR);	

			II) per i dipendenti, mediante una o più delle seguenti opzioni: • contratto/accordo individuale e distinto che prevede sanzioni o clausola nel contratto di lavoro che prevede sanzioni, o • politiche interne che prevedono sanzioni, o • contratti collettivi che prevedono sanzioni, o • altri mezzi (ma il gruppo deve spiegare in maniera adeguata come le BCR sono rese vincolanti per i dipendenti).	
A LIVELLO ESTERNO				
1.3 Creazione di diritti del terzo beneficiario per gli interessati, inclusa la possibilità di proporre reclamo alle autorità di controllo competenti e di proporre ricorso alle autorità giurisdizionali	SI	SI	I) Diritti direttamente opponibili nei confronti del responsabile del trattamento: Le BCR devono conferire agli interessati diritti per far valere le BCR in qualità di terzi beneficiari direttamente nei confronti del responsabile del trattamento qualora le disposizioni in questione siano specificatamente dirette ai responsabili del trattamento, conformemente al regolamento. A tal riguardo, gli interessati devono perlomeno essere in grado di far valere i seguenti elementi delle BCR direttamente nei confronti del responsabile del trattamento: • obbligo di rispettare le istruzioni del responsabile del trattamento riguardanti il trattamento dei dati, anche riguardo al trasferimento di dati verso paesi terzi (articolo 28, paragrafo 3, lettera a), articolo 28, paragrafo 3, lettera g) e articolo 29 del regolamento, nonché la sezione 1.1, 6.1.II e 6.1.IV dei presenti criteri di riferimento); • obbligo di mettere in atto	

			misure di sicurezza tecniche e organizzative adeguate (articolo 28, paragrafo 3, lettera c) e articolo 32 del regolamento, nonché sezione 6.1.IV dei presenti criteri di riferimento) e obbligo di segnalare qualsiasi violazione di dati personali al titolare del trattamento (articolo 33, paragrafo 2, del regolamento e sezione 6.1.IV dei presenti criteri di riferimento); • obbligo di rispettare le condizioni quando si ricorre a un subresponsabile del trattamento sia all'interno che al di fuori del gruppo (articolo 28, paragrafo 2, articolo 28, paragrafo 3, lettera d); articolo 28, paragrafo 4, articoli 45, 46 e 47 del regolamento, nonché sezione 6.1.VI e 6.1.VII. dei presenti criteri di riferimento; • obbligo di assistere e di cooperare con il titolare del trattamento per conformarsi e dimostrare la conformità alla legge, ad esempio nel dare seguito alle richieste degli interessati riguardanti i loro diritti (articolo 28, paragrafo 3, lettera e), articolo 28, paragrafo 3, lettera f), articolo 28, paragrafo 3, lettera h), e sezioni 3.2, 6.1.I, 6.1.III, 6.1.IV, 6.1.V e 6.1. 2 dei presenti criteri di riferimento); • facile accesso alle BCR (articolo 47, paragrafo 2, lettera g), del regolamento, e sezione 1.8 dei presenti criteri di riferimento); • diritto di proporre reclamo attraverso i meccanismi interni di reclamo (articolo 47, paragrafo 2, lettera i), e	

			sezione 2.2 dei presenti criteri di riferimento); • obbligo di cooperare con l'autorità di controllo (articolo 31, articolo 47, paragrafo 2, lettera l), del regolamento, e sezione 3.1 dei presenti criteri di riferimento); • disposizioni in materia di responsabilità, risarcimento e giurisdizione (articolo 47, paragrafo 2, lettera e), articolo 79, articolo 82 del regolamento, e sezioni 1.3, 1.5 e 1.7 dei presenti criteri di riferimento); • legislazione nazionale che impedisce il rispetto delle BCR (articolo 47, paragrafo 2, lettera m), e sezione 6.3 dei presenti criteri di riferimento). II) Diritti opponibili nei confronti del responsabile del trattamento nel caso in cui l'interessato non sia in grado di proporre reclamo nei confronti del titolare del trattamento: Le BCR devono conferire espressamente agli interessati diritti per far valere le BCR in qualità di terzi beneficiari nel caso in cui l'interessato non sia in grado di proporre reclamo nei confronti del titolare del trattamento, poiché quest'ultimo è scomparso di fatto, ha giuridicamente cessato di esistere o è divenuto insolvente, a meno che tutti gli obblighi del titolare del trattamento siano stati trasferiti, per contratto o per legge, all'eventuale successore, nel qual caso l'interessato può far valere i suoi diritti nei confronti del successore. In tal caso, gli interessati devono perlomeno essere in grado di far	

			valere nei confronti del responsabile del trattamento le seguenti sezioni di cui ai presenti criteri di riferimento: 1.1, 1.3, 1.5, 1.7, 1.8, 2.2, 3.1, 3.2, 6.1, 6.2, 6.3. I diritti degli interessati menzionati ai paragrafi I) e II) devono comprendere i ricorsi giurisdizionali per qualsiasi violazione dei diritti garantiti al terzo beneficiario e il diritto di ottenere riparazione e, ove opportuno, un risarcimento per il pregiudizio subito (danno materiale, così come qualsiasi tipo di disagio). In particolare, agli interessati deve essere concesso il diritto di proporre reclamo a un'autorità di controllo competente (scelta tra l'autorità di controllo dello Stato membro dell'UE in cui risiedono abitualmente, lavorano oppure del luogo ove si è verificata la presunta violazione) e ricorso alle autorità giurisdizionali competenti dello Stato membro dell'UE (possibilità dell'interessato di promuovere un'azione dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare o il responsabile del trattamento ha uno stabilimento o l'interessato risiede abitualmente, conformemente all'articolo 79 del regolamento). Qualora il titolare e il responsabile del trattamento coinvolti nello stesso trattamento siano considerati responsabili dell'eventuale danno causato da tale trattamento, all'interessato deve essere concesso il diritto di ottenere un risarcimento per l'intero ammontare del danno direttamente dal responsabile del trattamento (articolo 82, paragrafo 4, del regolamento).	

1.4. Responsabilità nei confronti del titolare del trattamento	SI	SI	È opportuno rendere vincolanti le BCR nei confronti del titolare del trattamento specificandolo nell'accordo di servizio che quest'ultimo dovrà essere conforme all'articolo 28 del regolamento. Le BCR devono inoltre stabilire che il titolare del trattamento deve avere il diritto di far valere le BCR nei confronti di qualsiasi membro vincolato dalle BCR per le violazioni commesse da quest'ultimo, nonché nei confronti dei membri vincolati dalle BCR di cui al punto 1.5 in caso di violazione delle BCR o dell'accordo di servizio da parte dei membri vincolati dalle BCR stabiliti al di fuori dell'UE, oppure in caso di violazione dell'accordo scritto di cui al punto 6.1.VII da parte di qualsiasi sub-responsabile esterno del trattamento stabilito al di fuori dell'UE.	
1.5 L'impresa accetta di assumersi la responsabilità di pagare il risarcimento e di porre rimedio alle violazioni delle BCR	SI	SI	Le BCR devono includere l'obbligo per le sedi principali nell'UE del responsabile del trattamento o per il membro vincolato dalle BCR stabilito nell'UE del responsabile del trattamento con responsabilità delegate di protezione dei dati, oppure per il responsabile del trattamento dell'esportatore dell'UE (ad es., la parte UE che stipula un contratto con il titolare del trattamento) di accettare di assumersi la responsabilità e di concordare di intraprendere le azioni necessarie per porre rimedio agli atti di altri membri vincolati dalle BCR stabiliti al di fuori dell'UE o alle violazioni compiute da un sub-responsabile esterno del trattamento stabilito al di fuori	

			dell'UE, nonché di pagare un risarcimento per gli eventuali danni causati dalla violazione delle BCR. Il membro vincolato dalle BCR accetterà di assumersi la responsabilità come se la violazione fosse stata causata da lui stesso nello Stato membro in cui ha sede anziché dal membro vincolato dalle BCR stabilito al di fuori dell'UE o da un sub-responsabile esterno del trattamento che ha sede al di fuori dell'UE. Il membro vincolato dalle BCR non può far valere la violazione degli obblighi ad opera del sub-responsabile del trattamento (interno o esterno al gruppo) al fine di escludere la propria responsabilità. Se per alcuni gruppi con strutture societarie particolari non è possibile imporre a un soggetto specifico di assumersi l'intera responsabilità per qualsiasi violazione delle BCR al di fuori dell'UE, un'altra opzione può prevedere che ogni membro vincolato dalle BCR che esporta dati al di fuori dell'UE sia responsabile delle violazioni delle BCR da parte di sub-responsabili del trattamento (interni o esterni al gruppo) stabiliti al di fuori dell'UE che hanno ricevuto i dati da tale membro vincolato dalle BCR stabilito nell'UE.	
1.6 L'impresa dispone di risorse sufficienti	NO	SI	Il modulo di domanda deve contenere la conferma che il membro vincolato dalle BCR che ha accettato di assumersi la responsabilità degli atti di altri membri vincolati alle BCR stabiliti al di fuori dell'UE e/o di qualsiasi sub-responsabile esterno del trattamento stabilito al	

			di fuori dell'UE dispone di risorse sufficienti per corrispondere i risarcimenti dei danni risultanti dalle violazioni delle BCR.	
1.7 L'onere della prova spetta all'impresa, non al singolo	SI	SI	Le BCR devono stabilire che al membro vincolato dalle BCR che ha accettato di assumersi la responsabilità spetti l'onere di dimostrare che il membro vincolato dalle BCR stabilito al di fuori dell'UE o che il sub-responsabile esterno del trattamento non è responsabile della violazione delle norme per la quale l'interessato chiede il risarcimento del danno. Le BCR devono inoltre stabilire che, nel caso in cui il titolare del trattamento possa dimostrare di aver subito danni e presentare i fatti che indicano che sia probabile che i danni siano stati causati dalla violazione delle BCR, spetterà al membro vincolato dalle BCR del gruppo che ha accettato di assumersi la responsabilità l'onere di dimostrare che il membro vincolato dalle BCR al di fuori dell'UE o il sub-responsabile esterno non era responsabile della violazione delle BCR che ha determinato tali danni o che tale violazione non ha avuto luogo. Se il soggetto che ha accettato di assumersi la responsabilità è in grado di dimostrare che il membro vincolato dalle BCR stabilito al di fuori dell'UE non è responsabile dell'evento, può ritenersi sollevato da qualunque responsabilità.	

1.8 Gli interessati possono accedere facilmente alle BCR e, in particolare, alle informazioni riguardanti i diritti garantiti al terzo beneficiario da cui possono trarre beneficio	SI	NO	Accesso del titolare del trattamento: tramite l'accordo di servizio verrà garantita la presenza delle BCR nel contratto. Le BCR saranno allegate all'accordo di servizio o vi sarà un riferimento ad esse con la possibilità di accedervi in formato elettronico. Accesso degli interessati: Le BCR devono contenere l'impegno secondo cui a tutti gli interessati che godono dei diritti del terzo beneficiario si dovrebbero fornire, in particolare, le informazioni riguardanti i loro diritti del terzo beneficiario relativi al trattamento dei dati personali che li riguardano e i mezzi per esercitare tali diritti. Le BCR devono garantire il diritto di ogni interessato di avere facile accesso alle stesse. Parti pertinenti delle BCR devono essere pubblicate sul sito web del gruppo dei responsabili del trattamento o comunicate tramite altri mezzi appropriati secondo modalità facilmente accessibili agli interessati, oppure, quantomeno, per mezzo di un documento che includa **tutte** le informazioni (e non una sintesi di queste) riguardanti i punti 1.1, 1.3, 1.4, 1.6, 1.7, 2.2, 3.1, 3.2, 4.1, 4.2, 6.1, 6.2, 6.3 dei presenti criteri di riferimento.	
2 - EFFICACIA				
2.1 Esistenza di un programma di formazione appropriato	SI	SI	Le BCR devono stabilire che sarà fornita una formazione appropriata sulle BCR al personale che ha accesso permanente o regolare ai dati personali, che è coinvolto nella raccolta dei dati personali o nello sviluppo di strumenti utilizzati per il trattamento dei dati personali.	

			Le autorità di controllo che valutano le BCR potranno richiedere alcuni esempi e spiegazioni del programma di formazione nel corso della procedura di domanda, e tale programma dovrà essere specificato nella domanda.	
2.2 Esistenza di un processo di gestione dei reclami per le BCR	SI	SI	Le BCR devono prevedere l'impegno da parte del gruppo dei responsabili del trattamento di creare un punto di contatto specifico per gli interessati. Tutti i membri vincolati alle BCR si impegnano a comunicare, senza ingiustificato ritardo, un reclamo o una domanda al titolare del trattamento, senza che siano obbligati a gestirli (salvo diversamente convenuto con il titolare del trattamento). Le BCR devono prevedere l'impegno da parte del responsabile del trattamento di gestire i reclami provenienti dagli interessati nel caso in cui il titolare del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente. In tutti i casi in cui sia il responsabile del trattamento a gestire i reclami, ciò deve avvenire senza ingiustificato ritardo e, in ogni caso, entro un mese, da parte di un reparto o di una persona chiaramente identificati che abbia un livello adeguato di indipendenza nell'esercizio delle proprie funzioni. Tenuto conto della complessità e del numero di domande, tale periodo può essere prorogato al massimo di altri due mesi, nel qual caso l'interessato dovrà esserne informato di conseguenza.	

			Il modulo di domanda deve spiegare il modo in cui gli interessati saranno informati delle fasi pratiche del sistema di reclamo, in particolare: • l'organo a cui proporre reclamo; • la forma in cui i reclami devono essere presentati; • i tempi per la risposta a un reclamo; • le conseguenze in caso di rigetto del reclamo; • le conseguenze nel caso in cui il reclamo sia considerato giustificato; • le conseguenze nel caso in cui l'interessato non sia soddisfatto delle risposte (diritto di proporre ricorso all'autorità giurisdizionale/ all'autorità di controllo).	
2.3 Esistenza di un programma di verifica esteso alle BCR	SI	SI	Le BCR devono istituire l'obbligo per il gruppo di prevedere verifiche sulla protezione dei dati su base periodica (da parte di revisori accreditati interni o esterni) o su richiesta specifica del responsabile/dell'ufficio competente per la tutela della vita privata (o di qualsiasi altra carica competente all'interno dell'organizzazione) al fine di garantire la verifica della conformità alle BCR. Le BCR devono stabilire che il programma di verifica riguardi tutti gli aspetti delle BCR, inclusi i metodi per assicurare provvedimenti correttivi. Devono inoltre stabilire che il risultato sia comunicato al responsabile/ all'ufficio per la tutela della vita privata e al consiglio di amministrazione competente della società controllante di un gruppo o del gruppo di	

			imprese che svolgono un'attività economica comune, e che sia reso accessibile anche al titolare del trattamento. Se del caso, il risultato potrà essere comunicato al consiglio di amministrazione della società madre. Le BCR devono stabilire che le autorità di controllo competenti per il titolare del trattamento possono avere accesso, su richiesta, ai risultati delle verifiche, e devono conferire loro l'autorità/la facoltà di effettuare esse stesse una verifica sulla protezione dei dati di qualsiasi membro vincolato dalle BCR, se necessario. Qualsiasi responsabile o sub-responsabile del trattamento incaricato del trattamento dei dati personali per conto di un particolare titolare del trattamento accetterà, su richiesta di quest'ultimo, di sottoporre i propri impianti di trattamento dei dati alla verifica delle attività di trattamento relative a tale titolare del trattamento che verrà svolta dal titolare del trattamento o da un organismo di controllo composto da membri indipendenti e in possesso delle necessarie qualificazioni professionali, vincolati da obbligo di riservatezza, selezionati dal titolare del trattamento dei dati, eventualmente di concerto con l'autorità di controllo. Il modulo di domanda conterrà una descrizione del sistema di verifica. Ad esempio: • il soggetto (reparto all'interno del gruppo) che decide il piano/programma di verifica; • il soggetto che conduce l'attività di verifica;	

			• la frequenza dell'attività di verifica (periodica o su richiesta specifica dell'ufficio competente in materia di tutela della vita privata); • ambito della verifica (ad esempio, applicazioni, sistemi informatici, banche dati che trattano dati personali o trasferimenti successivi, decisioni adottate riguardo alle disposizioni vincolanti della legislazione nazionale che sono in contrasto con le BCR, la verifica delle clausole contrattuali per i trasferimenti fuori dal gruppo (verso titolari del trattamento o responsabili del trattamento), provvedimenti correttivi, ecc.); • il soggetto che riceve i risultati delle attività di verifica.	
2.4 Creazione di una rete di responsabili della protezione dei dati o personale adeguato preposto al monitoraggio della conformità alle norme	SI	NO	Le BCR dovrebbero prevedere un impegno a designare un responsabile protezione dei dati, ove richiesto, in linea con l'articolo 37 del regolamento, o una qualsiasi altra persona o soggetto (quale un responsabile della vita privata) avente la responsabilità di monitorare la conformità alle BCR. Tale persona/soggetto godrà del massimo supporto gestionale nell'esercizio delle sue funzioni. Il responsabile della protezione dei dati o un'altra persona/soggetto menzionati può essere assistito, rispettivamente, nell'esercizio delle sue funzioni, da una squadra/una rete di responsabili della protezione dei dati o contatti locali, a seconda del caso. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico (articolo 38, paragrafo 3, del regolamento).	

			Una breve descrizione della struttura interna, del ruolo, della posizione e dei compiti del responsabile della protezione dei dati o di una carica analoga menzionati e della squadra/ rete creata per garantire la conformità alle norme. Ad esempio, indicare che il responsabile della protezione dei dati o il responsabile della vita privata fornisce informazioni e consulenza al vertice gerarchico, si occupa delle indagini delle autorità di controllo, monitora e riferisce annualmente sulla conformità alle BCR a livello globale, e che i responsabili della protezione dei dati o i contatti locali sono incaricati di riferire sulle questioni di maggiore rilevanza in materia di vita privata al responsabile della protezione dei dati o al responsabile della vita privata e di monitorare la formazione e la conformità a livello locale.	
3 - OBBLIGO DI COOPERAZIONE				
3.1 Obbligo di cooperazione con le autorità di controllo	SI	SI	Le BCR devono includere l'obbligo chiaro per tutti i membri vincolati dalle BCR di cooperare con le autorità di controllo competenti per il titolare del trattamento pertinente, di accettare di essere controllati dalle stesse e di conformarsi a quanto raccomandato da tali autorità riguardo a qualsiasi aspetto connesso alle norme.	
3.2 Obbligo di cooperazione con il titolare del trattamento	SI	SI	Le BCR devono includere l'obbligo chiaro per qualsiasi responsabile o sub-responsabile del trattamento di cooperare e assistere il titolare del trattamento per conformarsi	

			alla legislazione sulla protezione dei dati (come, ad esempio, l'obbligo di rispettare i diritti degli interessati o di gestire i loro reclami, oppure essere in grado di rispondere a inchieste o indagini compiute dalle autorità di controllo). Ciò deve essere effettuato a tempo debito e nella misura del possibile.	
4 - DESCRIZIONE DEL TRATTAMENTO E DEI FLUSSI DI DATI				
4.1 Descrizione dei trasferimenti e campo di applicazione materiale delle BCR	SI	SI	Le BCR devono contenere un elenco dei membri vincolati dalle BCR, ossia dei soggetti vincolati dalle BCR (cfr. anche il punto 6.2). Il responsabile del trattamento che presenta una BCR deve fornire all'autorità di controllo una descrizione generale dell'ambito di applicazione materiale delle BCR (natura prevista dei dati trasferiti, categorie di dati personali, il tipo di interessati dai trasferimenti, i tipi di trattamento previsti e relative finalità).	
4.2 Indicazione dell'ambito geografico delle BCR (natura dei dati, tipo di interessati, paesi)	SI	SI	Le BCR dovrebbero specificare la struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e di ciascuno dei membri vincolati dalle BCR. Le BCR devono indicare che è compito del titolare del trattamento applicare le BCR a: I) tutti i dati personali trattati per le attività dei responsabili del trattamento e soggetti al diritto dell'UE (ad esempio, i dati sono stati trasferiti a partire dall'Unione europea), OPPURE II) tutti i dati trattati per le attività dei responsabili del trattamento all'interno del gruppo a prescindere dall'origine dei dati.	

5 - MECCANISMI PER RIFERIRE E REGISTRARE LE MODIFICHE				
5.1 Processo per l'aggiornamento delle BCR	SI	SI	Le BCR possono essere modificate (ad esempio, per tenere conto di modifiche del contesto normativo o della struttura societaria) ma devono imporre l'obbligo di segnalare le modifiche a tutti i membri vincolati dalle BCR, alle autorità di controllo interessate, tramite l'autorità di controllo competente, e al titolare del trattamento. Nel caso in cui le condizioni di trattamento dovessero essere modificate, è opportuno informarne il titolare del trattamento in modo così tempestivo da permettere a quest'ultimo di opporsi a tale modifica o di recedere dal contratto prima che la modifica in questione venga effettuata (ad esempio, informare riguardo a qualsiasi cambiamento previsto per l'aggiunta o la sostituzione di subcontraenti, prima che i dati vengano comunicati al nuovo sub-responsabile del trattamento). Le BCR o l'elenco dei membri vincolati dalle BCR possono essere aggiornati senza che sia necessario presentare una nuova domanda di approvazione a condizione che: I) una persona o una squadra/ reparto identificati tenga un elenco completamente aggiornato dei membri vincolati dalle BCR e dei sub-responsabili del trattamento coinvolti nelle attività di trattamento dei dati per conto del titolare del trattamento che deve essere reso accessibile al titolare del trattamento dei dati, agli interessati e alle autorità di controllo;	

			II) tale persona conservi registrazioni degli aggiornamenti delle norme e fornisca sistematicamente le informazioni necessarie al titolare del trattamento dei dati e, su richiesta, alle autorità di controllo; III) non sia effettuato alcun trasferimento a un nuovo membro vincolato dalle BCR finché quest'ultimo non sia effettivamente vincolato dalla BCR e possa garantirne il rispetto; IV) le eventuali modifiche delle BCR o dell'elenco dei membri vincolati dalle BCR siano comunicate una volta all'anno alle autorità di controllo interessate tramite l'autorità di controllo competente, con una breve spiegazione dei motivi che giustificano l'aggiornamento; V) sia comunicata prontamente alle autorità di controllo interessate, tramite l'autorità di controllo competente, qualsiasi modifica che comprometta il livello di protezione offerto dalle BCR o incida significativamente sulle BCR (per esempio, modifiche del carattere vincolante).	
6 - GARANZIE DI PROTEZIONE DEI DATI				
6.1 Descrizione dei principi sul rispetto della vita privata, incluse le norme sui trasferimenti o trasferi-	SI	SI	Le BCR devono includere i seguenti principi che devono essere osservati da ogni membro vincolato dalle BCR: I) <u>trasparenza, correttezza e liceità</u>: i responsabili o i sub-responsabili del trattamento avranno l'obbligo generale di aiutare e assistere il titolare del trattamento nell'intento di conformarsi alla legge (ad	

menti successivi al di fuori dell'UE			esempio, essere trasparenti circa le attività dei sub-responsabili del trattamento per permettere al titolare del trattamento di informare correttamente l'interessato); II) <u>limitazione delle finalità</u>: obbligo di trattare i dati personali solo per conto del titolare del trattamento e conformemente alle sue istruzioni documentate, anche in caso di trasferimento di dati personali verso un paese terzo, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima che il trattamento venga effettuato, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico (articolo 28, paragrafo 3, lettera a), del regolamento). In altri casi, responsabile del trattamento non possa, per qualsiasi ragione, ottemperare a tale disposizione, si impegna a informarne prontamente il titolare del trattamento dei dati, nel qual caso quest'ultimo ha la facoltà di sospendere il trasferimento dei dati e/o di risolvere il contratto. Al termine della fornitura di servizi legati al trattamento dei dati, i responsabili e i sub-responsabili del trattamento provvedono, a scelta del titolare del trattamento, a cancellare o a restituire a quest'ultimo tutti i dati personali trasferiti e cancellare le relative copie, certificando al titolare del	

			trattamento, e si impegneranno affinché quest'ultimo garantisca la riservatezza dei dati personali e si astenga dal trattare di propria iniziativa tali dati; III) qualità dei dati: i responsabili e i sub-responsabili del trattamento avranno l'obbligo generale di aiutare e assistere il titolare del trattamento nell'intento di conformarsi alle legge. In particolare: • i responsabili e i sub-responsabili del trattamento eseguiranno tutte le misure necessarie su richiesta del titolare del trattamento, con l'intento di aggiornare, correggere o cancellare i dati. I responsabili e i sub-responsabili del trattamento informeranno ogni membro vincolato dalle BCR, ai quali sono stati comunicati i dati, di qualsiasi rettifica o cancellazione dei dati; • i responsabili e i sub-responsabili del trattamento eseguiranno tutte le misure necessarie su richiesta del titolare del trattamento, con l'intento di cancellare o rendere anonimi i dati dal momento in cui il modulo di identificazione non è più necessario. Il responsabile e i sub-responsabili del trattamento informeranno ogni soggetto a cui sono stati comunicati i dati di qualsiasi cancellazione o anonimizzazione dei dati; IV) sicurezza: i responsabili e i sub-responsabili del trattamento avranno l'obbligo di attuare tutte le misure tecniche e organizzative appropriate per assicurare	

			un livello di sicurezza adeguato ai rischi presentati dal trattamento, come previsto dall'articolo 32 del regolamento. I responsabili e i sub-responsabili del trattamento avranno inoltre l'obbligo di assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del regolamento, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento (articolo 28, paragrafo 3, lettera f), del regolamento). I responsabili e i sub-responsabili del trattamento devono mettere in atto misure tecniche e organizzative che rispondano quantomeno ai requisiti della legislazione applicabile al titolare del trattamento dei dati e qualsiasi misura particolare esistente nell'accordo di servizio. I responsabili del trattamento informano il titolare del trattamento, senza ingiustificato ritardo, dopo essere venuti a conoscenza della violazione dei dati personali. Inoltre, i sub-responsabili del trattamento hanno l'obbligo di informare il responsabile e il titolare del trattamento, senza ingiustificato ritardo, dopo essere venuti a conoscenza di qualsiasi violazione di dati personali; V) diritti degli interessati: i responsabili e i sub-responsabili del trattamento eseguiranno tutte le misure tecniche e organizzative appropriate, nella misura del	

			possibile, quando richiesto dal titolare del trattamento, al fine di soddisfare gli obblighi di quest'ultimo di dare seguito alle richieste per l'esercizio dei diritti degli interessati di cui al capo III del regolamento (articolo 28, paragrafo 3, lettera e), del regolamento), comunicando, tra l'altro, qualsiasi informazione utile che possa aiutare il titolare del trattamento ad adempiere all'obbligo di rispettare i diritti degli interessati. Il responsabile e i sub-responsabili del trattamento trasmetteranno al titolare del trattamento qualsiasi richiesta degli interessati senza rispondervi, salvo autorizzazione; VI) subcontratti all'interno del gruppo: il trattamento dei dati può essere delegato ad altri membri vincolati dalle BCR solo tramite previa autorizzazione informata scritta, specifica o generale, del titolare del trattamento[3]. L'accordo di servizio specificherà se sarà sufficiente un'autorizzazione preventiva generale fornita all'inizio del servizio oppure se sarà necessaria un'autorizzazione specifica per ogni nuovo sub-responsabile del trattamento. Se viene concessa un'autorizzazione generale, il titolare del trattamento dovrebbe essere informato dal responsabile del trattamento di qualsiasi cambiamento previsto riguardante l'aggiunta o la sostituzione di un sub-responsabile del trattamento in modo così	

			tempestivo da permettere al titolare del del trattamento di opporsi a tale modifica o di recedere dal contratto prima che i dati vengano comunicati al nuovo sub-responsabile; VII) <u>trasferimenti successivi a sub-responsabili del trattamento esterni</u>: il trattamento dei dati può essere delegato a membri non vincolati dalle BCR solo tramite previa autorizzazione informata scritta, specifica o generale, del titolare del trattamento[4]. Se viene concessa un'autorizzazione generale, il titolare del trattamento dovrebbe essere informato dal responsabile del trattamento di qualsiasi cambiamento previsto riguardante l'aggiunta o la sostituzione di sub-responsabili del trattamento in modo così tempestivo da permettere al titolare del trattamento di opporsi a tale modifica o di recedere dal contratto prima che i dati vengano comunicati al nuovo sub-responsabile. Laddove il membro vincolato dalle BCR affidi in subcontratto l'esecuzione degli obblighi ai sensi dell'accordo di servizio, con il consenso del titolare del trattamento, deve stipulare, a tal fine, con il sub- responsabile, un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri che garantisca un livello adeguato di protezione ai sensi degli articoli 28, 29, 32, 45, 46, 47 del regolamento e che faccia in modo che gli stessi obblighi in materia di protezione dei dati stabiliti nell'accordo	

			di servizio tra il titolare del trattamento e il responsabile del trattamento, nonché nelle sezioni 1.3, 1.4, 3 e 6 dei presenti criteri di riferimento, siano imposti al sub-responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento (articolo 28, paragrafo 4, del regolamento).	
6.1.2 Responsabilizzazione e *altri strumenti*	SI	SI	I responsabili del trattamento avranno l'obbligo di mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28, paragrafo 3, lettera h), del regolamento, e consentiranno e contribuiranno alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato. Inoltre, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati. Al fine di dimostrare la conformità con le BCR, i membri vincolati dalle BCR devono tenere un registro di tutte le categorie di attività di trattamento svolte per conto di ogni titolare del trattamento, in linea con i requisiti stabiliti all'articolo 30, paragrafo 2, del regolamento. Tale registro dovrebbe essere tenuto in forma scritta, anche in formato elettronico, e, su richiesta, essere	

			messo a disposizione dell'autorità di controllo (articolo 30, paragrafi 3 e 4, del regolamento). I membri vincolati dalle BCR devono inoltre assistere il titolare del trattamento nell'attuazione di misure tecniche e organizzative appropriate per il rispetto dei principi relativi alla protezione dei dati e per facilitare la conformità ai requisiti stabiliti dalle BCR nella prassi, come la protezione dei dati fin dalla progettazione e la protezione per impostazione definita (articolo 25 e articolo 47, paragrafo 2, lettera d), del regolamento).	
6.2 Elenco dei soggetti vincolati dalle BCR	SI	SI	Le BCR devono contenere un elenco dei soggetti vincolati dalle BCR, incluse le coordinate di contatto.	
6.3 Necessità di trasparenza nei casi in cui la legislazione nazionale impedisca al gruppo di conformarsi alle BCR	SI	NO	Un impegno chiaro secondo cui, qualora un membro vincolato dalle BCR abbia motivo di ritenere che la legislazione applicabile esistente o futura gli impedisca di rispettare le istruzioni ricevute dal titolare del trattamento o di ottemperare agli obblighi derivanti dalle BCR o dall'accordo di servizio, lo comunichi tempestivamente al titolare del trattamento che ha la facoltà di sospendere il trasferimento dei dati e/o di risolvere il contratto, al responsabile del trattamento della sede principale dell'UE, a un membro dell'UE con responsabilità delegate di protezione dei dati o all'altro responsabile/ufficio competente per la protezione della vita provata, nonché all'autorità di controllo competente per il titolare del trattamento e a quella	

			competente per il responsabile del trattamento. Qualsiasi richiesta giuridicamente vincolante di comunicazione di dati personali presentata da un'autorità giudiziaria o da un servizio di sicurezza nazionale deve essere comunicata al titolare del trattamento, salvo che ciò sia proibito da norme specifiche (come, ad esempio, da norme di diritto penale a tutela del segreto delle indagini). In ogni caso, la richiesta di comunicazione dovrebbe essere sospesa e l'autorità di controllo competente per il titolare del trattamento e quella per il responsabile del trattamento dovrebbero essere chiaramente informate di tale richiesta, comprese le informazioni sui dati richiesti, sull'organo richiedente e sulla base giuridica della comunicazione (salvo che ciò sia vietato da norme specifiche). Se, in casi specifici, la sospensione e/o la segnalazione sono vietate, le BCR devono prevedere che il membro vincolato dalle BCR si adoperi per ottenere il diritto di rinuncia al divieto al fine di comunicare quanto prima la maggiore quantità di informazioni, e sia in grado di dimostrare di aver agito in tal senso. Se, nei casi di cui sopra, nonostante tutti gli sforzi, il membro vincolato dalle BCR non si trovi nella posizione di poter informare l'autorità di controllo competente, esso deve impegnarsi nelle BCR a fornire annualmente all'autorità di controllo competente informazioni generali sulle richieste ricevute (per esempio, numero di richieste di comunicazione, tipo di dati richiesti, richiedente se possibile, ecc.).	

			In ogni caso, le BCR devono stabilire che i trasferimenti di dati personali da un membro del gruppo vincolato dalle BCR all'autorità pubblica non possono essere massicci, sproporzionati e indiscriminati da andare oltre quanto necessario in una società democratica.	
6.4 Specificazione del rapporto tra il diritto nazionale e le BCR	SI	NO	Le BCR devono specificare il loro rapporto con il diritto applicabile in materia. Le BCR devono stabilire che, qualora il diritto locale, ad esempio quello dell'UE, richieda un livello di protezione dei dati personali più elevato, tale diritto prevalga sulle BCR. I dati personali saranno trattati in ogni caso secondo il diritto applicabile.	

II. IMPEGNI DA ASSUMERE NELL'ACCORDO SUL LIVELLO DEL SERVIZIO

Le BCR per i responsabili del trattamento devono essere legate in maniera inequivocabile all'accordo sul livello del servizio firmato con ogni cliente. A tal fine, è importante assicurarsi che, nell'accordo sul livello del servizio, che deve contenere tutti gli elementi richiesti di cui all'articolo 28 del regolamento:

- le BCR siano rese esecutive per il titolare del trattamento (cliente) tramite uno specifico riferimento nell'accordo sul livello di servizio (SLA) (in allegato);
- il titolare del trattamento si impegni affinché, se il trasferimento riguarda categorie particolari di dati, l'interessato venga informato, prima del trasferimento, del fatto che i suoi dati potrebbero essere trasmessi a un paese terzo non in grado di fornire una protezione adeguata;
- il titolare del trattamento si impegni inoltre ad informare l'interessato dell'esistenza di responsabili del trattamento situati al di fuori dell'UE e non vincolati dalle BCR; il titolare del trattamento deve mettere a disposizione degli interessati, su richiesta, una copia delle BCR e dell'accordo di servizio (senza che vi sia alcuna informazione commerciale sensibile e riservata);
- vengano descritte misure di riservatezza e di sicurezza chiare, a cui si può fare riferimento tramite un link elettronico;
- venga fornita una descrizione chiara delle istruzioni e del trattamento dei dati;
- l'accordo di servizio specifichi se i dati possono essere oggetto di trattamento da parte di sub-responsabili all'interno o all'esterno del gruppo e se l'autorizzazione preventiva espressa dal titolare del trattamento sia generale o debba essere attribuita in modo specifico ogni nuova attività di trattamento affidata a sub-responsabili.

NOTE

[1] Documento di lavoro WP204: Explanatory Document on the Processor Binding Corporate Rules (documento esplicativo sulle norme vincolanti d'impresa per i responsabili del trattamento), versione emendata e adottata il 22 maggio 2015.

[2] Documento di lavoro WP 195a: Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities (Raccomandazione 1/2012 sul modulo di domanda standard per l'approvazione delle norme vincolanti d'impresa per il trasferimento di dati personali nel quadro di attività di trattamento), adottata il 17 settembre 2012.

[3] Informazioni sugli elementi principali (parti, paesi, sicurezza, garanzie in caso di trasferimenti internazionali, con la possibilità di ottenere una copia dei contratti impiegati). Informazioni dettagliate riguardanti, ad esempio, il nome dei sub-responsabili, potrebbero essere fornite, ad es., in un registro pubblico digitale.

[4] Informazioni sugli elementi principali (parti, paesi, sicurezza, garanzie in caso di trasferimenti internazionali, con la possibilità di ottenere una copia dei contratti impiegati). Informazioni dettagliate riguardanti, ad esempio, il nome dei sub-responsabili, potrebbero essere fornite, ad es., in un registro pubblico digitale.

Documento di lavoro che stabilisce una procedura di cooperazione per l'approvazione di "norme vincolanti d'impresa" per titolari e responsabili del trattamento ai sensi del RGPD (*) [WP 263 rev. 01]

Adottato l'11 aprile 2018

INTRODUZIONE

La procedura di approvazione di norme vincolanti d'impresa (*Binding Corporate Rules*, o BCR) per titolari e responsabili del trattamento è fissata nelle disposizioni di cui agli artt. 47, paragrafo 1, 63, 64 e (solo ove necessario) 65 del Regolamento (Ue) 2016/679 (RGPD).
Conseguentemente, le norme vincolanti d'impresa devono essere approvate dall'autorità di controllo competente[1] nel singolo Stato membro conformemente al meccanismo di coerenza di cui all'art. 63, in base al quale il Comitato europeo della protezione dei dati (CEPD) emette un parere non vincolante sul progetto di decisione sottopostogli dall'autorità di controllo competente (art. 64 RGPD).
Poiché i soggetti appartenenti al gruppo imprenditoriale che presenti una richiesta di approvazione per le rispettive BCR possono essere localizzati in più di uno Stato membro, la procedura in questione può coinvolgere più autorità di controllo interessate (SA)[2], per esempio quelle dei paesi di provenienza dei dati oggetto dei trasferimenti previsti. Tuttavia, il RGPD non prevede norme specifiche per la fase di cooperazione che dovrebbe aver luogo fra le SA precedentemente alla sottoposizione del progetto di decisione al CEPD, né fissa regole specifiche ai fini dell'individuazione della SA competente – che fungerà da Autorità Capofila per le BCR ("Capofila BCR")[3]. La Capofila BCR dovrà, fra l'altro, fungere da punto unico di contatto con il gruppo o l'ente richiedente l'approvazione durante la relativa procedura e occuparsi anche della procedura stessa nella fase di cooperazione.
Il presente documento si prefigge di aggiornare il documento WP107 individuando procedure di cooperazione snelle ed efficaci, conformi al RGPD, profittando appieno della pregressa e fruttuosa esperienza sviluppata dalle autorità di protezione dati nel processo di approvazione di BCR.
Si prevede di riesaminare e, ove necessario, aggiornare il presente documento sulla base dell'esperienza applicativa acquisita nel corso dell'implementazione del RGPD.

(*) *NDR. Traduzione a cura dell'Ufficio del Garante per la protezione dei dati personali del testo non disponibile in lingua italiana*

1. IDENTIFICAZIONE DELL'AUTORITÀ CAPOFILA PER LE BCR

1.1. Un gruppo imprenditoriale, ovvero un gruppo di imprese che svolge un'attività economica comune (il "Gruppo"), il quale intenda presentare un progetto di norme vincolanti d'impresa (BCR) ai fini dell'approvazione da parte dell'autorità competente conformemente agli artt. 47, 63 e 64 del RGPD dovrebbe proporre una SA in qualità di Capofila BCR. La decisione sulla SA che dovrebbe fungere da Capofila BCR si fonda sui criteri contenuti nel presente documento (si veda il paragrafo successivo). Spetta al singolo organismo o ente giustificare motivatamente la scelta di una specifica SA quale Capofila BCR.

1.2. Un gruppo che presenti la relativa richiesta di approvazione dovrebbe motivare la proposta relativa alla Capofila BCR sulla base di criteri pertinenti quali:
   a. la localizzazione della sede centrale del Gruppo in Europa;
   b. la localizzazione della società all'interno del Gruppo cui sono delegate le responsabilità in materia di protezione dei dati;[4]
   c. la localizzazione della società più idonea (in termini di funzioni gestionali, aggravio amministrativo, ecc.) a gestire la richiesta di approvazione e a dare attuazione alle norme vincolanti d'impresa all'interno del Gruppo;
   d. il luogo ove viene assunta la maggior parte delle decisioni in termini di finalità e strumenti del trattamento (ossia, del trasferimento); e
   e. lo Stato membro nell'Ue dal quale avrà origine la maggior parte o la totalità dei trasferimenti verso Paesi non appartenenti al SEE.

1.3. Si dovrà prestare particolare attenzione al criterio indicato al punto 1.2(a).

1.4. I criteri sopra elencati non hanno natura formale. La SA cui viene inviata la richiesta (in quanto candidata a fungere da Capofila BCR) sarà libera di decidere se essa rappresenti realmente la Capofila più idonea all'uopo e, in ogni caso, le SA possono decidere autonomamente di assegnare la richiesta a una SA diversa da quella cui inizialmente il Gruppo si era rivolto (si veda il paragrafo successivo), in particolare qualora ciò risulti fattibile e utile al fine di velocizzare la procedura (per esempio, tenuto conto del carico di lavoro cui deve far fronte la SA individuata inizialmente).

1.5. Il soggetto richiedente dovrà inoltre fornire alla Capofila BCR individuata come sopra (il punto di ingresso) tutte le opportune informazioni (in formato cartaceo ed elettronico, al fine di facilitarne l'ulteriore circolazione) a sostegno della proposta formulata, fra cui la natura e la configurazione generale delle attività di trattamento nell'Ue con particolare riguardo al luogo o ai luoghi ove sono assunte le decisioni in materia, alla sede e alla natura delle società collegate o consociate nell'Ue, al numero di dipendenti o di interessati dal trattamento, alle modalità e finalità del trattamento stesso, ai luoghi di origine dei trasferimenti diretti verso paesi terzi, e ai paesi terzi di destinazione dei dati oggetto di tali trasferimenti.

2. PROCEDURA DI COOPERAZIONE AI FINI DELL'APPROVAZIONE DI BCR

2.1. La Capofila BCR proposta nei modi sopra descritti inoltrerà a tutte le SA interessate[5] le informazioni ricevute in merito alle motivazioni della scelta operata dalla società quanto all'individuazione di quella specifica SA quale autorità capofila per le BCR, specificando anche se accetti o meno di fungere da Capofila BCR. Se il punto di ingresso accetta di fungere da Capofila BCR, alle altre SA interessate sarà chiesto, ai sensi dell'art. 57, paragrafo 1, lettera g) del RGPD, di manifestare eventuali obiezioni entro il termine di due settimane (termine prolungabile di due ulteriori settimane su richiesta di una SA interessata). Vale il principio del silenzio-assenso. Qualora il punto di ingresso non ritenga di poter fungere da Capofila BCR, dovrebbe spiegare le motivazioni di tale decisione e indicare (eventualmente) quale altra SA sarebbe a suo giudizio più idonea a fungere da autorità capofila. Le SA interessate si impegneranno a giungere a una decisione sul punto entro un mese dalla data in cui è stata fatta circolare inizialmente la pertinente documentazione.

2.2. Una volta stabilito quale sia la Capofila BCR, quest'ultima inizierà l'interazione con il soggetto che ha presentato la richiesta esaminando la documentazione relativa al progetto di BCR. Per favorire una maggiore coerenza, invierà (ai sensi dell'art. 57, paragrafo 1, lettera g), del RGPD) una prima revisione del progetto di BCR e della relativa documentazione a una o due SA (in rapporto al numero di Stati membri a partire dai cui territori avranno luogo i trasferimenti)[6] che fungeranno da co-revisori collaborando con la Capofila BCR nel processo di valutazione. Qualora non vi siano reazioni da una SA co-revisore entro un mese dalla data dell'invio del progetto di BCR e della relativa documentazione (termine prorogabile in presenza di giustificati motivi), si riterrà che tale SA acconsenta al progetto di BCR in questione. In taluni casi sarà necessario produrre più redazioni del testo di BCR o avere più interazioni fra il soggetto richiedente e le SA interessate prima di giungere a una versione finale soddisfacente.

2.3. L'esito del processo descritto dovrebbe essere un "progetto consolidato" di BCR che il soggetto richiedente invierà alla Capofila BCR, la quale lo farà circolare fra tutte le SA interessate[7] ai sensi dell'art. 57, paragrafo 1, lettera g) del RGPD per riceverne i commenti. In base alla procedura qui delineata, il termine per le osservazioni sul progetto consolidato di BCR non sarà superiore a 1 mese. Qualora una SA interessata non abbia sollevato obiezioni motivate entro il termine suddetto, si riterrà che tale SA acconsenta al progetto consolidato.

2.4. La Capofila BCR invierà al soggetto richiedente ogni ulteriore commento sul "progetto consolidato" e, se necessario, può continuare l'interazione con il richiedente. Se l'autorità capofila ritiene che quest'ultimo sia in grado di dare un seguito soddisfacente a tutti i commenti ricevuti, lo inviterà a sottoporle un "progetto finale" di BCR.

2.5. Ai sensi dell'art. 64, paragrafo 1, del RGPD, la capofila BCR presenterà al Comitato il progetto di decisione relativo al "progetto finale" di BCR unitamente a tutte le informazioni pertinenti, la documentazione e le

opinioni delle SA interessate. Il CEPD adotterà un parere in merito conformemente all'Art. 64, paragrafo 3, RGPD e al suo Regolamento interno.

2.6. Qualora il parere reso dal CEPD ai sensi dell'art. 64, paragrafo 3, confermi il progetto di decisione sul progetto di BCR nella forma sottoposta al Comitato stesso, la Capofila BCR adotterà la sua decisione approvando il progetto di BCR.

2.7. Qualora il parere reso dal CEPD ai sensi dell'art. 64, paragrafo 3, richieda modifiche del progetto di BCR, la Capofila BCR comunicherà al Presidente del Comitato entro il periodo di due settimane di cui all'art. 64, paragrafo 7, se intende mantenere invariato il progetto di decisione (ossia, se non intende conformarsi al parere del CEPD) oppure modificarlo nei termini indicati dal parere del CEPD[8]. Nel primo caso, ai sensi dell'art. 64, paragrafo 8, del RGPD, si applica l'art. 65, paragrafo 1, del RGPD[9]. Qualora la Capofila BCR comunichi al Presidente del Comitato l'intenzione di modificare il progetto di decisione nei termini di cui al parere del Comitato stesso, contatterà immediatamente il soggetto richiedente per chiedere che il progetto di BCR sia emendato in tal senso così da perfezionarne il testo. Una volta che il progetto di BCR sia stato perfezionato conformemente al parere del CEPD, la Capofila BCR modificherà in tale ottica il progetto iniziale di decisione, notificherà la decisione così modificata al CEPD come previsto dall'art. 64, paragrafo 7, e approverà le BCR.

2.8. Una volta che la Capofila BCR abbia approvato le BCR, ne informerà tutte le SA interessate cui farà pervenire una copia. Ai sensi dell'art. 46, paragrafo 2, lettera b), del RGPD, le "norme vincolanti d'impresa" così approvate forniranno le garanzie adeguate di cui al paragrafo 1 dell'art. 46 senza necessitare di alcuna autorizzazione specifica da parte delle altre autorità di controllo interessate.

2.9. Traduzioni: In via generale e salve eventuali ulteriori esigenze di traduzione, anche sulla base di previsioni normative, tutti i documenti compreso il progetto consolidato di BCR dovrebbero essere tradotti a cura del soggetto richiedente nella lingua della Capofila BCR e in inglese, ove possibile ai sensi del diritto nazionale. Il progetto finale e le BCR approvate devono essere tradotti a cura del soggetto richiedente nelle lingue delle SA interessate[10].

2.10. Una volta che le BCR siano state approvate, la Capofila BCR, conformemente ai documenti WP256 e WP257, punto 5.1, informerà le SA interessate di ogni aggiornamento riguardante le BCR o l'elenco dei membri vincolati da tali BCR fornito dal soggetto richiedente. Qualora il Gruppo ampliasse l'ambito delle BCR a un ulteriore Stato membro dell'Ue (a seguito dello stabilimento di un nuovo membro vincolato dalle BCR in tale ulteriore Stato membro), la SA di tale ultimo Stato membro sarà una SA interessata ai fini del punto 2.8 di cui sopra.

NOTE

[1] L'art. 57, paragrafo 1, lettera s) del RGPD prevede quanto segue: "Fatti salvi gli altri compiti indicati nel presente regolamento, sul proprio territorio ogni autorità di controllo (...) approva le norme vincolanti d'impresa ai sensi dell'articolo 47". Inoltre, ai sensi dell'art. 58, paragrafo 3, lettera j), del RGPD, ciascuna autorità di controllo ha "i poteri autorizzativi e consultivi (...) di approvare le norme vincolanti d'impresa ai sensi dell'articolo 47."

[2] Ai sensi dell'art. 4, n. 22, lettere (a) e (b), per "autorità di controllo interessata" si intende un'autorità di controllo interessata dal trattamento di dati personali in quanto il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; oppure in quanto gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento. Per quanto riguarda la procedura di approvazione di BCR, le SA interessate sono le SA dei paesi di provenienza dei dati oggetto di trasferimento, secondo quanto specificato dai richiedenti, ovvero, nel caso delle BCR-P, tutte le SA (poiché un responsabile del trattamento stabilito in uno Stato membro può fornire servizi a titolari situati in più Stati membri, e potenzialmente in tutti gli Stati membri).

[3] In linea di principio, la "Capofila BCR" è diversa dalla "Capofila OSS", ossia dall'autorità capofila nella procedura di sportello unico, tenendo conto del fatto che i trasferimenti contemplati nelle BCR non soddisfano solitamente i criteri definitori di ciò che configura un "trattamento transfrontaliero". Tuttavia, potrebbero verificarsi situazioni in cui la stessa SA agisce sia da Capofila BCR sia da Capofila OSS – per esempio qualora un trasferimento effettuato a partire da un solo stabilimento incida in modo sostanziale su interessati in più di uno Stato membro, ossia qualora dati personali siano inviati inizialmente dagli Stati membri A, B e C allo stabilimento del titolare nello Stato membro A, e successivamente trasferiti da tale stabilimento nello Stato membro A verso un Paese terzo o, nel caso di BCR-P, qualora il responsabile effettui gli stessi trasferimenti per tutti i clienti nei singoli Stati membri. In ogni caso, la procedura di approvazione delle BCR sarebbe quella specificamente prevista dall'articolo 64 del RGPD.

[4] In base all'art. 47, paragrafo 2, lettera f), del RGPD, deve esservi sempre un membro del Gruppo stabilito nel territorio di uno Stato membro che si assume la responsabilità per qualunque violazione delle norme vincolanti d'impresa commesse da un membro interessato non stabilito nell'Unione. Se la sede centrale del Gruppo fosse localizzata altrove, essa dovrebbe delegare tale responsabilità a un membro stabilito nell'Ue.

[5] Si veda la nota a piè di pagina n. 2, supra.

[6] Di regola la Capofila BCR si consulterà con 2 autorità in funzione di co-revisori qualora almeno 14 Stati membri siano interessati dai trasferimenti. Al di sotto di questa soglia è possibile fare affidamento su un solo co-revisore o su due co-revisori a seconda delle specificità del caso e della disponibilità manifestata dalle SA.

[7] V. nota a piè di pagina 1, supra.

[8] In base all'art. 64, paragrafo 5, il Presidente del Comitato fornisce, senza ingiustificato ritardo, con mezzi elettronici ogni informazione in merito ai membri del Comitato e alla Commissione.

[9] In particolare, ai sensi dell'art. 65, paragrafo 1, lettera c), "Al fine di assicurare l'applicazione corretta e coerente del presente regolamento nei singoli casi, il comitato adotta una decisione vincolante nei seguenti casi: (...) c) se un'autorità di controllo competente (...) non si conforma al parere del comitato emesso a norma dell'articolo 64. In tal caso qualsiasi autorità di controllo interessata o la Commissione può comunicare la questione al comitato."

[10] Si vedano, sul punto, anche i documenti WP256 e 257, Paragrafi 1.7, in base ai quali "Le BCR devono prevedere il diritto di ogni interessato di accedere con facilità al loro testo".

Raccomandazione concernente il modulo di richiesta di approvazione di norme vincolanti d'impresa per titolari del trattamento ai fini del trasferimento di dati personali (*) [WP 264]

Adottato l'11 aprile 2018

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.
Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

(*) *NDR. Traduzione a cura dell'Ufficio del Garante per la protezione dei dati personali del testo non disponibile in lingua italiana*

MODULO DI RICHIESTA DI APPROVAZIONE DI NORME VINCOLANTI D'IMPRESA PER TITOLARI AI FINI DEL TRASFERIMENTO DI DATI PERSONALI[1]

INTRODUZIONE E ISTRUZIONI

Il Regolamento generale sulla protezione dei dati (UE) 2016/679 (RGPD) consente il trasferimento di dati personali al di fuori del SEE soltanto qualora il paese terzo garantisca un "livello adeguato di protezione" dei dati (art. 45) oppure qualora il titolare fornisca garanzie adeguate con riguardo alla tutela della vita privata (art. 46). Le norme vincolanti d'impresa (Binding Corporate Rules, BCR) costituiscono uno degli strumenti atti a dimostrare l'esistenza di tali garanzie adeguate (art. 47) da parte di un gruppo imprenditoriale o di un gruppo di imprese che svolgono un'attività economica comune.

Ai sensi dell'art. 64 RGPD, il ricorso a BCR quali garanzie adeguate ai fini di trasferimenti internazionali di dati dal SEE richiede l'approvazione dell'autorità di controllo competente nel rispetto del meccanismo di coerenza di cui all'art. 63, senza necessitare di una specifica autorizzazione da parte di un'autorità di controllo (art. 46, paragrafo 2, lettera b) RGPD). Il modulo si basa su documenti già pubblicati dal Gruppo di lavoro "Articolo 29" delle autorità europee per la protezione dei dati (il "Gruppo di lavoro"), in particolare il documento WP133, e mira a supportare i soggetti richiedenti l'approvazione nel dimostrare le modalità di adesione ai requisiti fissati nell'art. 47 RGPD e nel documento WP256.

ISTRUZIONI GENERALI

- È necessario compilare e presentare all'Autorità di controllo (SA) che si ritiene essere l'autorità capofila per le BCR ("Capofila BCR") una sola copia del modulo, nel rispetto degli artt. 47, paragrafo 1, e 64 RGPD e delle indicazioni contenute nel documento WP263; il modulo è utilizzabile in tutti gli Stati membri facenti parte del SEE.
- Compilare tutte le voci e presentare il modulo alla SA che si ritiene essere la Capofila BCR.
- È possibile aggiungere pagine ulteriori o inserire allegati se lo spazio per le risposte risulta insufficiente.
- È possibile specificare quali informazioni o materiali siano commercialmente sensibili e debbano, quindi, essere mantenuti riservati; tuttavia, si tenga presente che tale documentazione sarà fatta circolare fra le SA interessate e sottoposta al Comitato europeo della protezione dei dati (CEPD), al quale incombe di emettere un parere sul progetto di decisione di approvazione delle BCR, ai sensi dell'art. 64 RGPD. In ogni caso, le richieste di accesso a tali informazioni formulate da soggetti terzi saranno trattate da ciascuna autorità di controllo interessata nel rispetto della normativa nazionale.

- Le note in calce presenti nel modulo di richiesta indicano le disposizioni pertinenti dell'art. 47 RGPD e dei documenti del Gruppo di lavoro, WP256, nonché quelle contenute in specifici paragrafi dei documenti WP74 e WP108, ove sono forniti chiarimenti ulteriori che mantengono la propria validità nel quadro del RGPD.
- Una volta presentato il modulo, la SA cui ci si è rivolti farà circolare la Parte 1 del modulo a tutte le "autorità di controllo interessate"[2] per stabilire quale fra esse debba fungere da Capofila BCR.
- Sarà la SA cui ci si è rivolti a comunicare quale SA sia stata in ultimo designata dalle SA interessate a fungere da Capofila BCR.
- Di norma, la Capofila BCR chiederà l'assistenza di altre due SA interessate (co-revisori) al fine di valutare le BCR alla luce dell'art. 47 e del WP256[3].
- Una volta terminata la revisione, ai sensi dell'art. 64 RGPD la Capofila BCR farà circolare la parte rimanente del modulo, contenente le BCR, a tutte le altre autorità di controllo interessate così da raccoglierne le osservazioni e inviarle al Comitato europeo della protezione dei dati (CEPD) unitamente al progetto di parere sulle BCR.

PARTE 1 - INFORMAZIONI SUL SOGGETTO RICHIEDENTE

Sezione 1: Struttura e coordinate di contatto relative al richiedente e al gruppo imprenditoriale, o al gruppo di imprese che svolgono un'attività economica in comune ("Gruppo")

- Se la sede centrale del Gruppo è nel SEE, occorre che il modulo sia compilato e presentato dalla sede centrale nel SEE.
- Se la sede centrale del Gruppo è situata al di fuori del SEE, il Gruppo dovrebbe designare un membro all'interno del SEE (preferibilmente nel paese della Capofila BCR potenziale) quale membro del Gruppo con "responsabilità delegate in materia di protezione dei dati". È questo soggetto che dovrà poi presentare la richiesta per conto del Gruppo.
- Coordinate di contatto del responsabile in caso di quesiti:
  - Indicare un responsabile cui rivolgere eventuali quesiti concernenti la richiesta.
  - Il responsabile suddetto può trovarsi al di fuori del SEE, anche se per praticità ciò non sarebbe consigliabile.
  - È possibile indicare un contatto funzionale e non una persona specifica.

Sezione 2: Descrizione sintetica dei flussi di dati

- Il soggetto richiedente dovrebbe descrivere sinteticamente l'ambito e la natura dei flussi di dati in uscita dal SEE rispetto ai quali si chiede l'approvazione delle BCR.

Sezione 3: Individuazione della Capofila BCR

- Conformemente all'art. 64 RGPD, la Capofila BCR è l'autorità incaricata di coordinare l'approvazione delle BCR presentate, che potranno quindi essere considerate garanzie adeguate nei paesi SEE indicati nella richiesta dai quali originano trasferimenti di dati personali da parte di membri del

Gruppo verso paesi terzi, senza necessitare di una specifica autorizzazione all'impiego delle BCR rilasciata dalle altre autorità di controllo interessate.

- Prima di rivolgersi a una SA in quanto presunta Capofila BCR, è bene analizzare i fattori di cui alla Sezione 1 del documento WP263 (gli stessi già elencati alle Sezioni 3.3. e 3.4 del documento WP108). Alla luce di tali fattori occorre illustrare, nella Parte 1.3 della richiesta, quale SA dovrebbe fungere da Capofila BCR. Le SA non sono obbligate ad accettare l'indicazione espressa nella richiesta, se ritengono che un'altra SA possa fungere più adeguatamente da Capofila BCR, in particolare se ciò consentisse di velocizzare la procedura (per esempio, tenendo conto del carico di lavoro cui già soggiace la SA inizialmente individuata).

PARTE 2 - DOCUMENTAZIONE DI RIFERIMENTO

Sezione 4: Vincolatività delle norme vincolanti d'impresa

- Ai fini dell'approvazione delle BCR per il trasferimento di dati personali, occorre dimostrarne l'efficacia giuridicamente vincolante sia internamente (fra i membri del Gruppo, e con riguardo a dipendenti e sub-contraenti) sia esternamente (a beneficio delle persone fisiche i cui dati personali sono trattati dal Gruppo) nel rispetto della legislazione nazionale. Queste domande servono a ottenere le informazioni necessarie a stabilire se le BCR presentate abbiano la suddetta efficacia vincolante.
- Nella richiesta occorre chiarire che l'onere della prova con riguardo a presunte violazioni delle norme ricadrà su un membro del Gruppo stabilito nel territorio di uno Stato membro (per esempio, quello da cui ha origine il trasferimento, oppure in cui si trova la sede centrale ovvero quella parte dell'organizzazione con responsabilità delegate in materia di protezione dati), a prescindere dal luogo di origine del reclamo.
- Le autorità di regolazione competenti per determinati settori (per esempio, i servizi finanziari) potrebbero vietare a un membro del Gruppo situato in un certo paese di farsi carico della responsabilità in capo a un diverso membro del Gruppo in un altro paese. Se tale condizione si verificasse nel caso della richiesta presentata, si dovranno fornire le informazioni pertinenti nella sottosezione denominata "Reclami e ricorsi giurisdizionali" illustrando ogni altro meccanismo implementato dal Gruppo per garantire che le persone abbiano modo di far valere le proprie doglianze nei confronti del Gruppo nel SEE.

Sezione 5: Efficacia

- Per dimostrare l'efficacia (ossia verificare l'osservanza) si può fare ricorso a numerosi meccanismi tipicamente utilizzati all'uopo dalle aziende, per esempio programmi che prevedano audit su base regolare, attività di governance aziendale, l'istituzione di servizi deputati alla compliance, ecc. Si prega di rispondere alle domande concernenti l'efficacia tenendo presenti i meccanismi di verifica dell'osservanza utilizzati nel gruppo.
- Sarà necessario confermare la possibilità per le SA interessate nel SEE di condurre audit della compliance.

Sezione 6: Cooperazione con le SA

- La Sezione 6 riguarda la cooperazione con le SA. Occorre specificare in che modo le BCR affrontano il tema della cooperazione con le SA.

Sezione 7: Descrizione dei trattamenti e dei flussi di dati

- Al fine di consentire alle SA di valutare se le BCR offrano garanzie adeguate per i trasferimenti di dati ai sensi dell'art. 47 RGPD, è fondamentale descrivere i flussi di dati all'interno del Gruppo in modo completo e comprensibile.

Sezione 8: Meccanismi per la segnalazione e la registrazione delle modifiche

- Tanto le SA quanto i membri del Gruppo devono essere informati senza ingiustificato ritardo di eventuali modifiche delle BCR. In particolare, devono essere comunicate tempestivamente alle SA interessate, tramite la SA competente ai sensi dell'art. 64 (ossia, la Capofila BCR)[4], le modifiche che incidono in misura significativa sull'osservanza delle norme relative alla protezione dei dati (ossia, che incidono sui diritti degli interessati), a differenza delle modifiche di natura esclusivamente amministrativa (tranne ove queste ultime incidano sulle BCR – per esempio, in caso di modifiche della loro vincolatività). In questa sezione occorre descrivere i meccanismi implementati dal Gruppo per segnalare e registrare le suddette modifiche.
- L'obbligo di segnalazione delle modifiche si applica soltanto con riguardo al testo delle BCR vere e proprie, e non alla documentazione di corredo, a meno che una modifica apportata a tale documentazione incida in misura significativa sull'osservanza delle BCR.

Sezione 9: Garanzie per la protezione dei dati

- In questa sezione si dovranno specificare i meccanismi previsti nelle BCR per dare attuazione alle garanzie essenziali in materia di protezione dei dati che sono necessarie a offrire un livello adeguato di tutela dei dati oggetto di trasferimento.

Allegato 1: Testo ufficiale delle norme vincolanti d'impresa

- Allegare copia delle BCR. Non deve trattarsi necessariamente di un documento unico, potendo le BCR essere costituite da più documenti. In quest'ultimo caso occorre specificare quali rapporti intercorrano in termini giuridici fra i singoli documenti: per esempio, norme generali - norme specifiche riferite a uno specifico settore, come la gestione risorse umane o la gestione clientela.
- Non occorre allegare tutta la documentazione a corredo in questa fase; vi si potrà provvedere successivamente dopo l'interazione con la Capofila BCR.

MODULO DI RICHIESTA DI APPROVAZIONE DI NORME VINCOLANTI D'IMPRESA (BCR)

PARTE 1 - INFORMAZIONI SUL SOGGETTO RICHIEDENTE

1. STRUTTURA E COORDINATE DI CONTATTO RELATIVE AL GRUPPO IMPRENDITORIALE O AL GRUPPO DI IMPRESE CHE SVOLGONO UN'ATTIVITÀ ECONOMICA IN COMUNE (IL GRUPPO)

Denominazione del Gruppo e localizzazione della sede centrale:

……

La sede centrale del Gruppo si trova nel SEE?

☐ Sì

☐ No

Denominazione e localizzazione del soggetto richiedente:

……

Identificativo (ove esistente): ……..

Natura giuridica del soggetto richiedente (società di capitali, società di persone, ecc.) ……

Descrizione della posizione ricoperta dal soggetto richiedente all'interno del Gruppo: (p.es.: sede centrale del Gruppo nel SEE, oppure, se il Gruppo non ha una sede centrale nel SEE, membro del Gruppo nel SEE con responsabilità delegate in materia di protezione dei dati) ……

……

Nome e/o qualifica della persona che funge da contatto (Nota: la persona che funge da contatto può variare nel tempo, è possibile indicare coordinate funzionali anziché il nome di una persona specifica):

Indirizzo:……..

Stato: ……..

Telefono: …… Fax: …… E-Mail: ……

Stati membri nel SEE per i quali si farà uso delle BCR:

……

2. DESCRIZIONE SINTETICA DEL TRATTAMENTO E DEI FLUSSI DI DATI[5]

Specificare quanto segue:

- Natura dei dati coperti dalle BCR, in particolare se le BCR si applicano a una sola categoria di dati ovvero a più categorie; tipologia del trattamento e relative finalità; categorie di interessati (per esempio, dati relativi a dipendenti, clienti, fornitori e altri terzi nell'ambito delle ordinarie attività commerciali rispettivamente svolte,...)

.....

- Le BCR si applicano solo ai trasferimenti a partire dal SEE oppure a tutti i trasferimenti fra membri del Gruppo?

.....

- Specificare da quale paese sia trasferito al di fuori del SEE il maggiore volume di dati:

.....

- Ambito dei trasferimenti intra-Gruppo coperti dalle BCR; inserire la descrizione e le coordinate di contatto relative a membri del Gruppo all'interno o all'esterno del SEE cui possano essere trasferiti i dati personali

.....

3. INDIVIDUAZIONE DELL'AUTORITÀ DI CONTROLLO CAPOFILA ("CAPOFILA BCR")[6]

Illustrare quale Autorità debba fungere da Capofila BCR alla luce dei criteri seguenti:

- Localizzazione della sede centrale del Gruppo nel SEE

.....

- Qualora il gruppo non disponga di una sede centrale nel SEE, localizzazione nel SEE del membro del Gruppo con responsabilità delegate in materia di protezione dei dati

.....

- Localizzazione della società più idonea (in termini di funzioni gestionali, oneri amministrativi, ecc.) a gestire la richiesta e garantire l'applicazione delle BCR all'interno del Gruppo

.....

- Paese dove viene assunta la maggior parte delle decisioni quanto a finalità e strumenti del trattamento

.....

- Stati membri del SEE a partire dai quali avverrà la maggioranza dei trasferimenti al di fuori del SEE

.....

PARTE 2 - DOCUMENTAZIONE DI RIFERIMENTO[7]

4. VINCOLATIVITÀ DELLE NORME VINCOLANTI D'IMPRESA (BCR)

VINCOLATIVITÀ A LIVELLO INTERNO[8]

Vincolatività all'interno dei membri del Gruppo[9]

In che modo si realizza la vincolatività delle BCR per i membri del Gruppo?

☐ Misure o norme che hanno natura giuridicamente vincolante per tutti i membri del Gruppo

☐ Contratti o accordi intra-gruppo fra i membri del Gruppo

☐ Dichiarazioni o impegni unilaterali assunti o forniti dalla società controllante che hanno natura vincolante per gli altri membri del Gruppo (ciò è possibile solo se il membro aderente alle BCR che si assume tale responsabilità è situato in uno Stato membro che riconosce natura vincolante alle dichiarazioni unilaterali, e se tale membro è giuridicamente in grado di vincolare gli altri membri del Gruppo soggetti alle BCR)

☐ Altre modalità (solo se il Gruppo dimostra in che modo sia garantita la natura vincolante delle BCR) - specificare

.....

.....

.....

Illustrare in che modo i meccanismi sopra indicati siano giuridicamente vincolanti per i membri del Gruppo, nel senso della loro azionabilità da altri membri del Gruppo (in particolare la sede centrale dello stesso):

.....

.....

La vincolatività delle BCR a livello interno si estende all'intero Gruppo? (se alcuni membri del Gruppo debbano esserne esonerati, specificare in che modo e per quali ragioni)

.....

.....

Vincolatività per i dipendenti[10]

Il Gruppo può adottare una o più delle misure qui indicate per garantire che le BCR siano vincolanti per i dipendenti, ma l'elenco non ha natura esaustiva. Inserire le necessarie spiegazioni:

- Contratto di lavoro

.....

- Accordi collettivi (approvati da commissioni per l'impiego/altri enti)

.....

- Obbligo per il dipendente di sottoscrivere una dichiarazione o di attestare di aver letto le BCR o una policy interna in cui siano incorporate le BCR

.....

- Incorporazione delle BCR nelle policy aziendali pertinenti

.....

- Altre modalità (ma il Gruppo deve spiegare in maniera adeguata come sia realizzata la vincolatività delle BCR per i dipendenti)

.....

- Sanzioni disciplinari per inosservanza delle policy aziendali pertinenti, compreso il licenziamento in caso di violazioni

.....

Si prega di illustrare sinteticamente, fornendo anche la pertinente documentazione ricavata da policy, procedure o accordi di riservatezza, in che modo le BCR siano rese vincolanti per i dipendenti.

.....

Vincolatività per i sub-contraenti che trattano i dati[11]

Quali misure sono state adottate per imporre ai subcontraenti di applicare tutele per il trattamento di dati personali (p. es, attraverso il ricorso a obblighi inseriti nei contratti stipulati con tali contraenti)? Specificare:

.....

.....

Come sono disciplinate le conseguenze dell'inadempimento in tali contratti o altri strumenti giuridici ai sensi del diritto Ue o dello Stato membro?

.....

.....

Specificare le sanzioni previste per i subcontraenti in caso di inadempimento

.....

.....

VINCOLATIVITÀ A LIVELLO ESTERNO[12]

In che modo le norme hanno vincolatività esterna a beneficio di singoli interessati (diritti dei terzi beneficiari) o in che modo si prevede di conferire tali diritti? Per esempio, si può ipotizzare il conferimento di diritti del terzo beneficiario attraverso contratti o dichiarazioni unilaterali[13].

.....

.....

Mezzi di reclamo o di ricorso

Specificare in che modo si dà seguito agli obblighi previsti dagli artt. 47.2(e), 77, 79 e 82 RGPD[14]

.....

.....

Si prega di fornire conferma del fatto che il titolare del trattamento stabilito nel territorio di uno Stato membro (p.e. la sede centrale del Gruppo, o il membro del Gruppo con responsabilità delegate per la protezione dei dati nel SEE) ha preso le misure opportune per consentire il pagamento di un risarcimento da parte sua o del membro del Gruppo all'origine del trasferimento in caso di danni risultanti dalla violazione delle BCR, compiuta da qualsiasi membro del Gruppo; specificare anche in che modo si garantisce l'applicazione di tali misure.

.....

.....

Si prega di fornire conferma del fatto che l'onere della prova con riguardo a una presunta violazione delle BCR ricade sul membro del Gruppo all'origine del trasferimento, ovvero sulla sede centrale europea, o sul membro nel SEE con responsabilità delegate in materia di protezione dei dati, indipendentemente dal Paese di origine del reclamo.

.....

.....

5. EFFICACIA[15]

È importante dimostrare in che modo le BCR adottate siano rese efficaci nella prassi quotidiana, in particolare nei paesi non facenti parte del SEE ove i dati saranno trasferiti sulla base delle BCR stesse, poiché sarà un elemento significativo ai fini della valutazione dell'adeguatezza delle garanzie fornite.

.....

Formazione e sensibilizzazione (dipendenti)

- Programmi specifici di formazione

.....

- Verifiche per i dipendenti relative a BCR e norme sulla protezione dei dati

.....

- Le BCR sono comunicate a tutti i dipendenti online ovvero in formato cartaceo

.....

- Revisione e approvazione da parte di quadri di livello elevato all'interno dell'azienda

.....

- Come è configurata la formazione dei dipendenti al fine di consentire loro di individuare eventuali interazioni con la protezione dei dati, ossia per consentire loro di identificare l'applicabilità alle rispettive mansioni delle politiche pertinenti in materia di privacy e di prendere le misure conseguenti? (indipendentemente dalla localizzazione dei dipendenti, all'interno o meno del SEE)

.....

Processo di gestione dei reclami[16]

Le BCR prevedono un sistema per la gestione interna dei reclami al fine di conseguire l'osservanza delle norme?

.....

Descrivere il sistema di gestione dei reclami:

.....

Verifica dell'osservanza

Quali sono i meccanismi previsti dal Gruppo per verificare l'osservanza delle BCR da parte di ogni membro? (p. es., esistenza di un programma di audit, di un programma di compliance, ecc.)? Si prega di specificare:

.....

.....

Illustrare in che modo opera il programma di verifica o di compliance all'interno del Gruppo (p.es., fornire informazioni sui destinatari delle relazioni di verifica/audit e sul loro posizionamento all'interno della struttura del Gruppo).

.....

.....

Le BCR prevedono il ricorso a:

- un responsabile della protezione dei dati (RPD)? .....
- auditor interni? .....
- auditor esterni? .....
- l'associazione di auditor interni ed esterni? .....
- verifiche da parte di un'unità compliance interna? .....

Le BCR specificano se i meccanismi di verifica sono indicati con chiarezza in...

- un documento relativo agli standard di protezione dati .....
- altri documenti e audit connessi a procedure interne? .....

Rete di RPD o personale idoneo[17]

Confermare l'esistenza di una rete di RPD o di personale idoneo (p. es. una rete di *privacy officer*), supportata dai vertici aziendali, con il compito di vigilare e garantire la compliance con le BCR:

.....

Illustrare l'operatività della rete di RPD o *privacy officer*:

- Struttura interna:

.....

- Ruoli e responsabilità:

.....

6. COOPERAZIONE CON LE SA[18]

Specificare come si configura nelle BCR l'attività di cooperazione con le SA:

.....

Confermate di permettere alle SA interessate di condurre audit della compliance?

.....

Confermate che il Gruppo nella sua interezza e ciascuna società del Gruppo si conformerà alle indicazioni dell'autorità di controllo interessata concernenti l'interpretazione e l'applicazione delle BCR?

.....

7. DESCRIZIONE DEI TRATTAMENTI E DEI FLUSSI DI DATI[19]

Specificare quanto segue:

- Natura dei dati coperti dalle BCR (dati relativi al personale, ecc.) e in particolare se le BCR si applicano a una sola categoria di dati o a più di una categoria

.....

- Qual è la natura dei dati oggetto del trasferimento?

.....

- In via generale, quali sono la destinazione e la provenienza dei dati oggetto del trasferimento?

.....

- Quale tipologia di trattamenti e quali finalità sono collegate ai dati oggetto del trasferimento e coperti dalle BCR, e quale tipologia di trattamenti sono effettuati successivamente al trasferimento stesso?

.....

- Ambito dei trasferimenti intra-gruppo coperti dalle BCR, compresa la descrizione e le coordinate di contatto di membri del Gruppo nel SEE o al di fuori del SEE che siano destinatari dei dati

.....

Le BCR si applicano esclusivamente ai trasferimenti a partire dal SEE oppure a tutti i trasferimenti fra membri del Gruppo? Specificare:

.....

8. MECCANISMI PER LA SEGNALAZIONE E LA REGISTRAZIONE DELLE MODIFICHE[20]

Confermare e descrivere in che modo le BCR consentano di informare altri membri del Gruppo e le SA interessate, per il tramite della SA competente ai sensi dell'art. 64 (ossia, la Capofila BCR), di eventuali modifiche apportate alle BCR stesse e/o all'elenco dei membri aderenti alle BCR (in sintesi):

.....

Confermare l'esistenza di un sistema finalizzato a registrare eventuali modifiche apportate alle BCR.

.....

9. GARANZIE PER LA PROTEZIONE DEI DATI[21]

Specificare con riguardo alle BCR l'approccio implementato rispetto alle tematiche di seguito indicate, allegando la documentazione pertinente ove opportuno:

• Trasparenza, correttezza, liceità

.....

• Limitazione della finalità

.....

• Minimizzazione ed esattezza dei dati

.....

• Periodo limitato di conservazione

.....

• Trattamento di categorie particolari di dati personali

.....

• Sicurezza, compreso l'obbligo di stipulare contratti con tutti i sub-contraenti/responsabili interni ed esterni nel rispetto di tutti i requisiti di cui all'art. 28, paragrafo 3, RGPD nonché dell'obbligo di notificare, senza ingiustificato ritardo, eventuali violazioni dei dati personali alla sede centrale in Ue o al membro in Ue aderente alle BCR con responsabilità delegate in materia di protezione dei dati, coinvolgendo anche le altre funzioni pertinenti / i privacy officer e informando gli interessati qualora la violazione possa comportare un rischio elevato per i loro diritti e libertà

.....

• Limitazioni poste ai trasferimenti ulteriori

.....

• Altro (p.es. misure a tutela dei minori, ecc.)

.....

10. RESPONSABILIZZAZIONE (ACCOUNTABILITY) E ALTRI STRUMENTI[22]

- Confermare e specificare in che modo i membri aderenti alle BCR saranno responsabili dell'osservanza delle BCR e in grado di dimostrarla

.....

- Confermare che i membri aderenti alle BCR terranno un registro di tutte le categorie di trattamenti svolti per conto di ciascun titolare, conformemente ai requisiti di cui all'art. 30, paragrafo 1, RGPD

.....

- Confermare che saranno condotte valutazioni di impatto sulla protezione dei dati con riguardo a trattamenti che possano presentare un rischio elevato per i diritti e le libertà di persone fisiche (RGPD art. 35), e che qualora una valutazione di impatto condotta ai sensi dell'art. 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare per ridurre tale rischio, si dovrebbe consultare l'autorità di controllo competente prima di procedere al trattamento (art. 36 RGPD)

.....

- Confermare e specificare quali misure tecniche e organizzative adeguate saranno implementate al fine di rispettare i principi di protezione dei dati e facilitare l'osservanza concreta dei requisiti fissati nelle BCR (p.es., protezione dei dati fin dalla fase di progettazione e per impostazione predefinita, art. 25 RGPD)

.....

Si prega di fornire la pertinente documentazione a supporto delle informazioni di cui sopra

.....

ALLEGATO 1:
TESTO UFFICIALE
DELLE NORME VINCOLANTI D'IMPRESA

Allegare copia delle BCR. Si noti che non è necessario allegare documentazione a corredo, quali policy privacy o norme privacy avente carattere specifico.

NOTE

[1] Il presente questionario tiene conto anche del progetto di modello di richiesta di approvazione di BCR elaborato dalla ICC (International Chamber of Commerce).

[2] Ai sensi dell'art. 4(22), lettera a) e b), per "autorità di controllo interessata" si intende un'autorità di controllo che è interessata dal trattamento di dati personali perché il titolare o il responsabile è stabilito nel territorio del rispettivo Stato membro, oppure perché "interessati che risiedono nello Stato membro di tale autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento". Per quanto concerne la procedura di approvazione di BCR, le SA interessate sono le SA dei paesi dai quali si prevede di effettuare i trasferimenti secondo quanto specificato dai richiedenti; nel caso di BCR-P, si tratta di tutte le SA (poiché un responsabile stabilito in uno Stato membro può fornire servizi a titolari situati in più Stati membri, e potenzialmente in tutti gli Stati membri).

[3] Di regola la Capofila BCR si consulterà con 2 autorità in funzione di co-revisori qualora almeno 14 Stati membri siano interessati dai trasferimenti. Al di sotto di questa soglia è possibile fare affidamento su un solo co-revisore o su due co-revisori a seconda delle specificità del caso e della disponibilità manifestata dalle SA.

[4] Si veda WP155, domanda 14.

[5] V. art. 47.2. a) e b), e Sezione 4.1. WP 256.

[6] V. Parte 1 WP 263.

[7] Documento di lavoro che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa, WP 256, adottato il 6 febbraio 2018.

[8] V. RGPD Art. 47.1.a) e 47.2.c), e Sezione 1.2 WP 256. V. anche le considerazioni di carattere generale contenute nella Sezione 3.3.1. WP74 e nella Sezione 5 WP108.

[9] V. Sezione 5.3 WP108.

[10] V. Art. 47.1.a), Sezione 1.2 WP 256 e Sezione 5.8 WP108.

[11] V. Art. 28.3 RGPD e Sezione 5.10 WP108.

[12] V. 47.1.b e) 47.2.c) ed e) RGPD e Sezione 1.3 WP 256. V. anche le considerazioni di carattere generale contenute nella Sezione 3.3.2 WP74.

[13] Gli interessati devono essere in grado di far valere almeno i seguenti elementi delle BCR:
- Principi in materia di protezione dei dati (Art. 47.2.d e Sezione 6.1 WP 256),
- Trasparenza e facile accesso alle BCR (Art. 47.2.g e Sezione 6.1 e 1.7 WP 256),
- Diritti di accesso, rettifica, cancellazione, limitazione del trattamento, opposizione al trattamento, diritto di non essere oggetto di decisioni basate esclusivamente su trattamenti automatizzati compresa la profilazione (RGPD Art. 47.2.e) e Artt. 15, 16, 17,18, 21, 22),
- Legislazione nazionale che impedisca l'osservanza delle BCR (Art. 47.2.m) e Sezione 6.3 del presente schema di riferimento),
- Diritto di proporre reclamo attraverso i meccanismi interni previsti dalla società (Art. 47.1.i) e Sezione 2.2 WP 256),
- Obblighi di cooperazione con l'autorità di controllo (Art. 47.2.k) e l), Sezione 3.1 WP 256),
- Disposizioni in materia di responsabilità e foro competente (Art. 47.2.e) e f), Sezioni 1.3, 1.4 WP 256).

Inoltre, si deve ricordare che il diritto civile di alcuni Stati non riconosce natura vincolante alle dichiarazioni unilaterali o agli impegni unilaterali. In assenza di una specifica disposizione normativa concernente la vincolatività di tali dichiarazioni, soltanto un contratto che contenga clausole del terzo beneficiario, stipulato fra i membri del Gruppo,

potrà comprovare la vincolatività in questione.

[14] Si veda anche la Sezione 1.3. WP 256: le BCR devono conferire il diritto di proporre reclamo all'autorità di controllo competente (scelta tra l'autorità di controllo dello Stato membro in cui si risiede abitualmente, si lavora oppure del luogo ove si è verificata la presunta violazione, ai sensi dell'articolo 77 del RGPD) e di proporre ricorso all'autorità giurisdizionale degli Stati membri dell'UE (possibilità per l'interessato di promuovere un'azione dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha sede o l'interessato risiede abitualmente, ai sensi dell'articolo 79 del RGPD).

[15] V. artt. 47.2.j e 47.2.l e art. 38.3 RGPD e Sezione 2.3 WP 256. V. anche le considerazioni di carattere generale contenute nella Sezione 5.2 WP74 e nella Sezione 6 WP108.

[16] V. artt. 47.2.i e 12.3 RGPD e Sezione 2.2 WP 256. V. anche Sezione 5.3 WP74.

[17] V. Sezione 2.4 WP 256.

[18] V. art. 47.2.l RGPD, Sezione 3.1 WP 256 e Sezione 5.4 WP 74.

[19] V. art. 47.2.b RGPD, Sezione 4.1 WP 256 e Sezione 7 WP108.

[20] V. art. 47.2.k RGPD e Sezione 5.1. WP 256.

[21] V. art. 47.2.d RGPD e Sezione 6.1. WP 256.

[22] V. Sezione 6.1.2 WP256.

Raccomandazione concernente il modulo di richiesta di approvazione di norme vincolanti d'impresa per responsabili del trattamento ai fini del trasferimento di dati personali (*) [WP 265]

Adottato l'11 aprile 2018

(*) *NDR. Traduzione a cura dell'Ufficio del Garante per la protezione dei dati personali del testo non disponibile in lingua italiana*

MODULO DI RICHIESTA DI APPROVAZIONE DI NORME VINCOLANTI D'IMPRESA (BCR) PER RESPONSABILI DEL TRATTAMENTO

PARTE 1 - INFORMAZIONI SUL SOGGETTO RICHIEDENTE

1. STRUTTURA E COORDINATE DI CONTATTO RELATIVE AL GRUPPO IMPRENDITORIALE O AL GRUPPO DI IMPRESE CHE SVOLGONO UN'ATTIVITÀ ECONOMICA IN COMUNE (IL GRUPPO)

Denominazione del Gruppo e localizzazione della sede centrale (società controllante):

……

La sede centrale del Gruppo si trova nel SEE?

☐ Sì

☐ No

Denominazione e localizzazione del soggetto richiedente:

……

Identificativo (ove esistente): ……..

Natura giuridica del soggetto richiedente (società di capitali, società di persone, ecc.) ……

……

Descrizione della posizione ricoperta dal soggetto richiedente all'interno del Gruppo: (p.es.: sede centrale del Gruppo nel SEE, oppure, se il Gruppo non ha una sede centrale nel SEE, membro del Gruppo nel SEE con responsabilità delegate in materia di protezione dei dati)

……

Nome e/o qualifica della persona che funge da contatto (Nota: la persona che funge da contatto può variare nel tempo, è possibile indicare coordinate funzionali anziché il nome di una persona specifica):

Indirizzo: ……..

Stato: ……..

Telefono: …… Fax: …… E-Mail: ……

Stati membri nel SEE per i quali si farà uso delle BCR per responsabili del trattamento:

……

2. DESCRIZIONE SINTETICA DEL TRATTAMENTO E DEI FLUSSI DI DATI

Specificare quanto segue:

- Natura dei dati coperti dalle BCR, in particolare se le BCR si applicano a una sola categoria di dati ovvero a più categorie; categorie di interessati (per esempio, dati relativi a dipendenti, clienti,...) tipologia del trattamento e relative finalità

.....

- Finalità previste dei trasferimenti per attività di trattamento

.....

- Le BCR si applicano solo ai trasferimenti a partire dal SEE oppure a tutti i trasferimenti per attività di trattamento fra membri del Gruppo?

.....

- Specificare da quale paese sia trasferito al di fuori del SEE il maggiore volume di dati per attività di trattamento:

.....

- Ambito dei trasferimenti intra-Gruppo coperti dalle BCR; inserire la descrizione e le coordinate di contatto relative a membri del Gruppo all'interno o all'esterno del SEE cui possano essere trasferiti i dati personali per attività di trattamento

.....

3. INDIVIDUAZIONE DELL'AUTORITÀ DI CONTROLLO CAPOFILA ("CAPOFILA BCR")

Illustrare quale Autorità debba fungere da Capofila BCR alla luce dei criteri seguenti:

- Localizzazione della sede centrale del Gruppo nel SEE

.....

- Qualora il gruppo non disponga di una sede centrale nel SEE, localizzazione nel SEE del membro del Gruppo con responsabilità delegate in materia di protezione dei dati

.....

- Localizzazione della società più idonea (in termini di funzioni gestionali, oneri amministrativi, ecc.) a gestire la richiesta e garantire l'applicazione delle BCR all'interno del Gruppo

.....

- Stati membri del SEE a partire dai quali avverrà la maggioranza dei trasferimenti al di fuori del SEE

.....

PARTE 2 - DOCUMENTAZIONE DI RIFERIMENTO[1]

4. VINCOLATIVITÀ DELLE NORME VINCOLANTI D'IMPRESA (BCR) PER RESPONSABILI DEL TRATTAMENTO

VINCOLATIVITÀ A LIVELLO INTERNO[2]

Vincolatività per i membri del Gruppo che agiscono in qualità di sub-responsabili interni[3]

In che modo si realizza la vincolatività delle BCR per i membri del Gruppo?

☐ Misure o norme che hanno natura giuridicamente vincolante per tutti i membri del Gruppo

☐ Contratti o accordi intra-gruppo fra i membri del Gruppo

☐ Dichiarazioni o impegni unilaterali assunti o forniti dalla società controllante che hanno natura vincolante per gli altri membri del Gruppo (ciò è possibile solo se il membro aderente alle BCR che si assume tale responsabilità è situato in uno Stato membro che riconosce natura vincolante alle dichiarazioni unilaterali, e se tale membro è giuridicamente in grado di vincolare gli altri membri del Gruppo soggetti alle BCR)

☐ Altre modalità (solo se il Gruppo dimostra in che modo sia garantita la natura vincolante delle BCR) - specificare

.....

.....

Illustrare in che modo i meccanismi sopra indicati siano giuridicamente vincolanti per i membri del Gruppo, nel senso della loro azionabilità da altri membri del Gruppo (in particolare la sede centrale dello stesso):

.....

La vincolatività delle BCR a livello interno si estende all'intero Gruppo? (qualora alcuni membri del Gruppo debbano esserne esonerati, specificare in che modo e per quali ragioni)

.....

Confermare che l'eventuale ricorso a sub-responsabili (interni) del trattamento è possibile solo previa informazione dei titolari del trattamento e sulla base del loro previo consenso per iscritto

.....

***Vincolatività per i dipendenti*[4]**

Il Gruppo può adottare una o più delle misure qui indicate per garantire che le BCR siano vincolanti per i dipendenti, ma l'elenco non ha natura esaustiva. Inserire le necessarie spiegazioni:

- Accordo/impegno individuale e distinto che prevede specifiche sanzioni

.....

- Contratto di lavoro che prevede specifiche sanzioni

.....

- Accordi collettivi (approvati da commissioni per l'impiego/altri enti) che prevedono specifiche sanzioni

.....

- Obbligo per il dipendente di sottoscrivere una dichiarazione o di attestare di aver letto le BCR per responsabili del trattamento o una policy interna in cui siano incorporate tali BCR

.....

- Incorporazione delle BCR nelle policy aziendali pertinenti unitamente alla previsione di sanzioni

.....

- Sanzioni disciplinari per inosservanza delle policy aziendali pertinenti, compreso il licenziamento in caso di violazioni

.....

- Altre modalità (ma il Gruppo deve spiegare in maniera adeguata come sia realizzata la vincolatività delle BCR per i dipendenti)

.....

Si prega di illustrare sinteticamente, fornendo anche la pertinente documentazione ricavata da policy, procedure o accordi di riservatezza, in che modo le BCR siano rese vincolanti per i dipendenti.

.....

VINCOLATIVITÀ A LIVELLO ESTERNO

Vincolatività per i sub-responsabili esterni che trattano i dati

Confermare che con i sub-responsabili esterni del trattamento viene stipulato un contratto per iscritto o altro atto giuridicamente valido ai sensi del diritto dell'Ue o dello Stato membro, il quale prevede una tutela adeguata in conformità degli artt. 28, 29, 32, 45, 46 e 47 RGPD e garantisce che i sub-responsabili esterni debbano rispettare gli stessi obblighi in materia di protezione dei dati che valgono per i membri del Gruppo ai sensi dei Contratti di servizio conclusi con i titolari e delle Sezioni 1.3, 1.4, 3 e 6 del WP257[5]:

.....

Come sono disciplinate le conseguenze dell'inadempimento in tali contratti o altri strumenti giuridici ai sensi del diritto Ue o dello Stato membro? Specificare le sanzioni previste per i sub-responsabili in caso di inadempimento.

.....

Confermare che il ricorso a sub-responsabili del trattamento (esterni) avviene solo previa autorizzazione informata e per iscritto del titolare, fornita in via specifica ovvero in via generale[6].

.....

Confermare che i sub-responsabili accettano, su richiesta di un titolare, di sottoporre ad audit gli strumenti utilizzati per i trattamenti di dati relativi a tale titolare[7]. Descrivere il sistema di audit.

.....

In che modo le norme hanno vincolatività esterna a beneficio di singoli interessati (diritti dei terzi beneficiari) o in che modo si prevede di conferire tali diritti? Per esempio, si può ipotizzare il conferimento di diritti del terzo beneficiario attraverso contratti o dichiarazioni unilaterali[8].

.....

Fornire una descrizione sintetica, supportata da estratti degli accordi sottoscritti con i titolari del trattamento, se del caso, delle modalità attraverso cui le BCR sono rese vincolanti nei confronti dei titolari del trattamento[9].

.....

Confermare che i diritti riconosciuti ai titolari comprendono il diritto di proporre ricorso in via giudiziaria e il diritto al risarcimento

.....

Mezzi di reclamo o di ricorso

Specificare in che modo si dà seguito agli obblighi previsti dagli artt. 47, paragrafo 2, lettera (e), 77, 79 e 82 RGPD, come ulteriormente specificati nel paragrafo 1.3 del documento WP257[10]

.....

Si prega di fornire conferma del fatto che il titolare di trattamento stabilito nel territorio di uno Stato membro (p.e. la sede centrale del Gruppo, o il membro del Gruppo del responsabile del trattamento con responsabilità delegate per la protezione dei dati nel SEE, o il responsabile esportatore nel SEE, cioè il soggetto situato nel SEE che ha stipulato il contratto con il titolare) ha preso le misure opportune per consentire il pagamento di un risarcimento da parte sua in caso di danni cagionati a un interessato o a un titolare e risultanti dalla violazione delle BCR compiuta da qualsiasi membro del Gruppo o da un sub-responsabile esterno; specificare anche in che modo si garantisce l'applicazione di tali misure.

.....

Si prega di fornire conferma del fatto che l'onere della prova con riguardo a una presunta violazione delle BCR causata da un membro del Gruppo o da un sub-responsabile esterno ricade sul membro del Gruppo in Ue che ha accettato di farsi carico della responsabilità di violazioni dovute a membri del Gruppo o a sub-responsabili del trattamento non situati nel SEE, indipendentemente dal Paese di origine del reclamo.

.....

Facile accesso alle BCR per responsabili del trattamento[11]

Si prega di fornire conferma del fatto che le BCR sono allegate ai contratti di servizio sottoscritti con i titolari del trattamento, o che a esse si fa rinvio con possibilità di accedervi elettronicamente:

.....

Si prega di fornire conferma del fatto che le BCR sono pubblicate sul sito del Gruppo responsabile del trattamento secondo modalità di facile accesso per gli interessati, o almeno che è pubblicato un documento contenente tutte le informazioni previste alla Sezione 1.8 del documento WP257:

.....

5. EFFICACIA[12]

È importante dimostrare in che modo le BCR adottate siano rese efficaci nella prassi quotidiana, in particolare nei paesi non facenti parte del SEE ove i dati saranno trasferiti sulla base delle BCR stesse, poiché sarà un elemento significativo ai fini della valutazione dell'adeguatezza delle garanzie fornite.

.....

Formazione e sensibilizzazione (dipendenti)[13]

- Programmi specifici di formazione

.....

- Verifiche per i dipendenti relative a BCR e norme sulla protezione dei dati

.....

- Le BCR sono comunicate a tutti i dipendenti online ovvero in formato cartaceo

.....

- Revisione e approvazione da parte di quadri di livello elevato all'interno dell'azienda

.....

- Come è configurata la formazione dei dipendenti al fine di consentire loro di individuare eventuali interazioni con la protezione dei dati, ossia per consentire loro di identificare l'applicabilità alle rispettive mansioni delle politiche pertinenti in materia di privacy e di prendere le misure conseguenti? (indipendentemente dalla localizzazione dei dipendenti, all'interno o meno del SEE)

.....

Processo di gestione dei reclami[14]

Le BCR prevedono un sistema per la gestione interna dei reclami al fine di (i) comunicare ai titolari senza ritardo eventuali reclami o richieste, e (ii) trattare reclami facendo le veci del titolare qualora quest'ultimo non sia più reperibile, abbia cessato di esistere o sia divenuto insolvente, ovvero qualora sia stato concordato con un titolare che il Gruppo si farà carico della trattazione di eventuali reclami e richieste da parte degli interessati?

.....

Descrivere il sistema di gestione dei reclami:

.....

Verifica dell'osservanza[15]

Quali sono i meccanismi previsti dal Gruppo per verificare l'osservanza delle BCR da parte di ogni membro? (p. es., esistenza di un programma di audit, di un programma di compliance, ecc.)? Si prega di specificare:

.....

Illustrare in che modo opera il programma di verifica o di compliance all'interno del Gruppo (p.es., fornire informazioni sui destinatari delle relazioni di verifica/audit e sul loro posizionamento all'interno della struttura del Gruppo).

.....

Le BCR per responsabili prevedono il ricorso a:

- un responsabile della protezione dei dati (RPD)? .....
- auditor interni? .....
- auditor esterni? .....
- l'associazione di auditor interni ed esterni? .....
- verifiche da parte di un'unità compliance interna? .....

Le BCR per responsabili specificano se i meccanismi di verifica sono indicati con chiarezza in...

- un documento relativo agli standard di protezione dati .....
- altri documenti e audit connessi a procedure interne? .....

Rete di RPD o personale idoneo[16]

Confermare l'esistenza di una rete di RPD o di personale idoneo (p. es. una rete di *privacy officer*), supportata dai vertici aziendali, con il compito di vigilare e garantire la compliance con le BCR per responsabili:

.....

Illustrare l'operatività della rete di RPD o *privacy officer*:
- Struttura interna:

.....

- Ruoli e responsabilità:

.....

6. COOPERAZIONE CON LE SA[17]

Specificare come si configura nelle BCR per responsabili l'attività di cooperazione con le SA:

.....

Confermate di permettere alle pertinenti SA di condurre audit della compliance?

.....

Confermate che il Gruppo nella sua interezza e ciascuna società del Gruppo si conformerà alle indicazioni delle pertinenti autorità di controllo quanto all'interpretazione e l'applicazione delle BCR per responsabili?

.....

7. COOPERAZIONE CON I TITOLARI DI TRATTAMENTO[18]

Specificare come si configura nelle BCR per responsabili l'attività di cooperazione con i titolari di trattamento:

.....

Confermate che accetterete di sottoporre i dispositivi di trattamento a un audit da parte del titolare (o di un ente ispettivo composto di membri indipendenti, individuato dal titolare) che ne abbia fatto richiesta, con riguardo ai trattamenti riferiti a tale titolare?

.....

8. DESCRIZIONE DEI TRATTAMENTI E DEI FLUSSI DI DATI[19]

Specificare quanto segue:

- Natura dei dati coperti dalle BCR per responsabili (dati relativi al personale, ecc.) e in particolare se le BCR si applicano a una sola categoria di dati o a più di una categoria

.....

- Qual è la natura dei dati oggetto del trasferimento ai fini di attività di trattamento?

.....

- In via generale, qual è l'ambito del flusso di dati?

.....

- Finalità per le quali i dati coperti dalle BCR per responsabili sono trasferiti verso Paesi terzi, e tipologia dei trattamenti

.....

- Ambito dei trasferimenti intra-gruppo coperti dalle BCR per responsabili, compresa la descrizione e le coordinate di contatto di membri del Gruppo nel SEE o al di fuori del SEE che possono ricevere dati personali per attività di trattamento

.....

Le BCR si applicano esclusivamente ai trasferimenti per attività di trattamento a partire dal SEE oppure a tutti i trasferimenti per attività di trattamento fra membri del Gruppo? Specificare:

.....

8. MECCANISMI PER LA SEGNALAZIONE E LA REGISTRAZIONE DELLE MODIFICHE[20](*)

Confermare e descrivere in che modo le BCR per responsabili consentano di informare altri membri del Gruppo, le SA interessate, per il tramite della SA competente ai sensi dell'art. 64 (ossia, la Capofila BCR), e i titolari di trattamento di eventuali modifiche apportate alle BCR stesse e/o all'elenco dei membri aderenti alle BCR (in sintesi):

.....

(*) *NDR. L'errata numerazione della tabella, con la ripetizione del n. 8, corrisponde alla versione ufficiale delle linee guida. Il documento è qui riproposto come nella versione originale.*

Confermare l'esistenza di un sistema finalizzato a registrare eventuali modifiche apportate alle BCR per responsabili

.....

Confermare che, in presenza di una modifica che incide sulle condizioni di trattamento, i titolari sono informati tempestivamente della possibilità di opporsi a tali modifiche o di risolvere il contratto prima dell'effettuazione della modifica in questione

.....

9. GARANZIE PER LA PROTEZIONE DEI DATI[21]

Specificare con riguardo alle BCR per responsabili l'approccio implementato rispetto alle tematiche di seguito indicate, allegando la documentazione pertinente ove opportuno:

- Trasparenza, correttezza, liceità (p.es., obbligo in via generale di fornire assistenza e supporto al titolare)

.....

- Limitazione della finalità (p.es., obbligo di trattare dati personali esclusivamente per conto del titolare e in conformità delle istruzioni da questo impartite, e di restituire i dati al titolare al termine della prestazione contrattuale)

.....

- Qualità dei dati (p.es., obbligo in via generale di fornire assistenza e supporto al titolare)

.....

- Sicurezza

.....

- Diritti degli interessati (p.es., obbligo in via generale di fornire assistenza e supporto al titolare)

.....

- Affidamento di trattamenti a sub-responsabili all'interno del Gruppo

.....

- Limitazioni poste ai trasferimenti ulteriori verso sub-responsabili esterni del trattamento

.....

- Altro (p.es. misure a tutela dei minori, ecc.)

.....

10. RESPONSABILIZZAZIONE (ACCOUNTABILITY) E ALTRI STRUMENTI[22]

- Confermare e specificare in che modo i membri aderenti alle BCR metteranno a disposizione del titolare tutte le informazioni necessarie a dimostrare l'osservanza dei rispettivi obblighi come previsti all'art. 28(3), lettera h), anche attraverso la conduzione di audit e la segnalazione al titolare di istruzioni che violino il RGPD o altre disposizioni nazionali o dell'Ue in materia di protezione dei dati.

.....

- Confermare che i membri aderenti alle BCR terranno un registro di tutte le categorie di trattamenti svolti per conto di ciascun titolare, conformemente ai requisiti di cui all'art. 30, paragrafo 2, RGPD.

.....

- Specificare in che modo i membri aderenti alle BCR supporteranno il titolare nell'implementazione di misure tecniche e organizzative adeguate al fine di rispettare i principi di protezione dei dati e facilitare l'osservanza concreta dei requisiti fissati nelle BCR (p.es., protezione dei dati fin dalla fase di progettazione e per impostazione predefinita)

.....

Si prega di fornire la pertinente documentazione a supporto delle informazioni di cui sopra

.....

ALLEGATO 1:
TESTO UFFICIALE
DELLE NORME VINCOLANTI D'IMPRESA PER RESPONSABILI

Allegare copia delle BCR per responsabili del trattamento. Si noti che non è necessario allegare documentazione a corredo, quali policy privacy o norme privacy aventi carattere specifico.

NOTE

[1] Documento di lavoro che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa per responsabili del trattamento, WP 257, adottato il 6 febbraio 2018.

[2] V. Sezione 1.1 e 1.2 WP 257.

[3] V. Sezione 1.2 (i) WP257.

[4] V. Sezione 1.2(ii) WP 257.

[5] V. Sezione 6.1 (vii) WP257.

[6] V. Sezione 6.1 (vii) WP257.

[7] V. Sezione 2.3 WP257.

[8] Si deve ricordare che il diritto civile di alcuni Stati (p.es., Italia, Spagna) non riconosce natura vincolante alle dichiarazioni unilaterali o agli impegni unilaterali. In assenza di una specifica disposizione normativa concernente la vincolatività di tali dichiarazioni, soltanto un contratto che contenga clausole del terzo beneficiario, stipulato fra i membri del Gruppo, potrà comprovare la vincolatività in questione.

[9] V. Sezione 1.4 WP257.

[10] Il paragrafo 1.3. del WP 257 prevede che le BCR devono conferire agli interessati il diritto in quanto terzi beneficiari di far valere le BCR nei confronti del responsabile, sia che i requisiti in oggetto siano diretti specificamente ai responsabili, conformemente al RGPD, sia quando l'interessato non è in grado di proporre un reclamo nei confronti del titolare del trattamento perché quest'ultimo si è reso irreperibile o ha cessato di esistere ovvero è in stato di insolvenza, a meno che un soggetto subentrante si sia fatto carico della totalità degli obblighi giuridicamente in capo al suddetto titolare in base a previsioni contrattuali o di legge, nel qual caso l'interessato potrà far valere i propri diritti nei confronti di tale ulteriore soggetto.

[11] V. Sezione 1.8 WP257

[12] V. Sezione 2 WP 257.

[13] V. Sezione 2.1 WP257

[14] V. Sezione 2.2 WP 257.

[15] V. Sezione 2.3 WP257.

[16] V. Sezione 2.4 WP 257.

[17] V. Sezione 3.1 WP 257.

[18] V. Sezione 3.2 WP 257.

[19] V. Sezione 4.1 WP 257.

[20] V. Sezione 5.1. WP 257.

[21] V. Sezione 6 WP 257.

[22] V. Sezione 6.1.2 WP257.

Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679

Adottate il 25 maggio 2018

Indice

visto l'articolo 70, paragrafo 1, lettera e) e lettera j), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

1. PARTE GENERALE

Il presente documento intende fornire una serie di orientamenti per l'applicazione dell'articolo 49 del regolamento generale sulla protezione dei dati (RGPD)[1] in merito alle deroghe relative al trasferimento di dati personali verso paesi terzi.

Il documento si basa sui precedenti elaborati[2] del gruppo di lavoro delle autorità per la protezione dei dati dell'UE, istituito in virtù dell'articolo 29 della direttiva sulla protezione dei dati (gruppo di lavoro "Articolo 29") e successivamente sostituito dal comitato europeo per la protezione dei dati (*European Data Protection Board* - EDPB), rispetto alle questioni cruciali derivanti dall'applicazione delle deroghe nell'ambito del trasferimento di dati personali verso paesi terzi. Il presente documento sarà rivisto e, se necessario, aggiornato sulla base dell'esperienza concreta acquisita con l'applicazione del RGDP.

Nell'applicare l'articolo 49 è opportuno ricordare che, ai sensi dell'articolo 44, l'esportatore di dati che trasferisca dati personali verso paesi terzi od organizzazioni internazionali è tenuto anche all'osservanza delle condizioni previste dalle altre disposizioni del RGDP. Ogni attività di trattamento deve essere conforme alle disposizioni pertinenti sulla protezione dei dati, segnatamente quelle degli articoli 5 e 6. Si rende pertanto necessaria una verifica articolata in due fasi: innanzitutto il trattamento dei dati deve essere fondato su una base giuridica, nel rispetto di tutte le disposizioni pertinenti di cui al RGDP; in secondo luogo occorre ottemperare alle disposizioni di cui al Capo V.

In virtù dell'articolo 49, paragrafo 1, in mancanza di una decisione di adeguatezza o di garanzie adeguate è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verificano determinate condizioni. Al contempo, l'articolo 44 impone l'applicazione di tutte le condizioni di cui al Capo V al fine di assicurare che il livello di protezione delle persone fisiche garantito dal RGPD non sia pregiudicato. Ciò significa che il ricorso alle deroghe dell'articolo 49 non deve mai portare a una violazione dei diritti fondamentali[3].

Il gruppo di lavoro "Articolo 29", predecessore del comitato europeo per la protezione dei dati, auspica da tempo, quale buona prassi, un approccio a più livelli[4] ai trasferimenti, che innanzitutto valuti se il paese terzo fornisce un livello di tutela adeguato e quindi assicuri che i dati esportati saranno protetti in quel paese. Se, tenuto conto delle circostanze, il livello di tutela non risultasse adeguato l'esportatore di dati deve valutare l'offerta di opportune garanzie. Pertanto in primo luogo gli esportatori devono esplorare la possibilità di collocare il trasferimento nell'ambito dei meccanismi di cui agli articoli 45 e 46 del RGPD e, soltanto qualora ciò non fosse possibile, possono ricorrere alle deroghe di cui all'articolo 49, paragrafo 1.

Le deroghe di cui all'articolo 49 sono pertanto eccezioni al principio generale secondo cui i dati personali possono essere trasferiti verso paesi terzi soltanto in presenza di adeguate garanzie nel paese terzo, oppure qualora siano state addotte garanzie adeguate e l'interessato goda di diritti effettivi e azionabili, affinché possa continuare a beneficiare dei diritti fondamentali e delle garanzie[5]. Per tali motivi, e in conformità con i principi del diritto europeo[6], le deroghe devono essere interpretate in maniera restrittiva, affinché l'eccezione non diventi la regola[7]. Tale posizione è confermata anche dalla formulazione del titolo dell'articolo 49, secondo cui le deroghe si applicano soltanto in situazioni specifiche ("Deroghe in specifiche situazioni").

Nel considerare il trasferimento di dati personali verso paesi terzi od organizzazioni internazionali gli esportatori di dati dovrebbero pertanto promuovere soluzioni che offrano agli interessati la garanzia di continuare a beneficiare, dopo il trasferimento, dei diritti fondamentali e delle garanzie cui hanno titolo in materia di trattamento dei dati. Poiché le deroghe non forniscono una tutela e garanzie adeguate per i dati personali trasferiti e poiché i trasferimenti fondati su una deroga non necessitano di alcuna autorizzazione preventiva dell'autorità di controllo, il trasferimento di dati personali verso paesi terzi sulla base delle deroghe comporta maggiori rischi per i diritti e per le libertà degli interessati.

Gli esportatori di dati devono essere consapevoli inoltre che, in mancanza di una decisione di adeguatezza, il diritto dell'Unione o degli Stati membri può, per importanti motivi di interesse pubblico, limitare espressamente il trasferimento di categorie specifiche di dati personali verso un paese terzo o un'organizzazione internazionale (articolo 49, paragrafo 5).

TRASFERIMENTI OCCASIONALI E NON RIPETITIVI

Il comitato europeo per la protezione dei dati osserva che il termine "occasionale" ricorre nel considerando 111 e l'espressione "non ripetitivo" ricorre nella deroga relativa agli "interessi legittimi cogenti" di cui all'articolo 49, paragrafo 1, comma 2. Tali espressioni indicano che i trasferimenti possono ripetersi ma non con cadenza regolare e devono avvenire in circostanze non ordinarie, ad esempio al manifestarsi di condizioni casuali o ignote e a intervalli di

tempo arbitrari. Un trasferimento di dati che si verifica con cadenza regolare nell'ambito di un rapporto stabile tra l'esportatore e un determinato importatore, per esempio, può essere sostanzialmente considerato sistematico e ripetuto e pertanto non presenta un carattere occasionale e non ripetitivo. Inoltre un trasferimento sarà generalmente considerato non occasionale o ripetitivo qualora, ad esempio, l'importatore di dati ottenga un accesso diretto generalizzato a una banca dati (ad esempio per mezzo di un'interfaccia a un'applicazione IT).

Il considerando 111 traccia una distinzione tra le deroghe dichiarando espressamente che in caso di "contratto" o "sede giudiziaria" (articolo 49, paragrafo 1, lettere b), c) ed e)) le deroghe si applicano esclusivamente a trasferimenti "occasionali", invece tale restrizione non sussiste qualora "l'interessato abbia esplicitamente acconsentito al trasferimento", in presenza di "importanti motivi di interesse pubblico", in caso di tutela degli "interessi vitali" e "in presenza di un registro", in virtù dell'articolo 49, paragrafo 1, lettere a), d), f) e g).

Occorre sottolineare tuttavia che anche le deroghe non espressamente limitate ai trasferimenti "occasionali" e "non ripetitivi" devono essere interpretate in modo da non contraddire la natura delle deroghe stesse, ossia eccezioni alla regola secondo la quale i dati personali possono essere trasferiti verso paesi terzi soltanto se il paese di destinazione offre un livello adeguato di protezione dei dati oppure, in alternativa, se sono messe in atto adeguate garanzie[8].

TEST DI NECESSITÀ

Un presupposto di fondo per il ricorso a varie deroghe risiede nella "necessità" del trasferimento di dati per una determinata finalità. Il test di necessità deve essere applicato per valutare la possibilità del ricorso alle deroghe di cui all'articolo 49, paragrafo 1, lettere b), c), d), e) ed f). Il test prevede che l'esportatore di dati nell'UE valuti se il trasferimento di dati personali possa essere considerato necessario per la finalità specifica della deroga da applicare. Per ulteriori informazioni sull'applicazione specifica del test per ciascuna deroga si rimanda alle sezioni corrispondenti riportate di seguito.

L'ARTICOLO 48 E LE DEROGHE

Il RGPD introduce una nuova disposizione nell'articolo 48, di cui bisogna tenere conto ai fini del trasferimento di dati personali. L'articolo 48 e il corrispondente considerando 115 dispongono che le decisioni di un'autorità amministrativa e le sentenze di un'autorità giurisdizionale di un paese terzo non costituiscono di per sé un motivo legittimo per il trasferimento di dati verso paesi terzi. Pertanto un trasferimento giustificato da una decisione delle autorità di un paese terzo risulta comunque illegittimo se non sono rispettatele condizioni di cui al Capo V[9].

Laddove sussista un accordo internazionale, quale un trattato bilaterale di mu-

tua assistenza giudiziaria, in linea generale le imprese dell'Unione dovrebbero rifiutare richieste dirette e rimandare l'autorità richiedente del paese terzo all'accordo o al trattato vigente.

Tale visione rispecchia fedelmente il disposto dell'articolo 44, che definisce un principio generale valido per tutte le disposizioni del Capo V al fine di garantire che il livello di protezione delle persone fisiche garantito dal RGPD non sia pregiudicato.

2. INTERPRETAZIONE SPECIFICA DELLE DISPOSIZIONI DI CUI ALL'ARTICOLO 49

2.1 L'INTERESSATO HA ESPLICITAMENTE ACCONSENTITO AL TRASFERIMENTO PROPOSTO, DOPO ESSERE STATO INFORMATO DEI POSSIBILI RISCHI DI SIFFATTI TRASFERIMENTI PER L'INTERESSATO, DOVUTI ALLA MANCANZA DI UNA DECISIONE DI ADEGUATEZZA E DI GARANZIE ADEGUATE - ARTICOLO 49, PARAGRAFO 1, LETTERA A)

Le condizioni generali alle quali il consenso può considerarsi valido sono definite all'articolo 4, paragrafo 11[10], e all'articolo 7 del RGPD[11]. Il gruppo di lavoro "Articolo 29" offre degli orientamenti in merito a tali condizioni in un documento separato, approvato dal comitato europeo per la protezione dei dati[12]. Le medesime condizioni per il consenso si applicano anche nell'ambito dell'articolo 49, paragrafo 1, lettera a). Sono tuttavia necessari ulteriori elementi specifici affinché il consenso possa considerarsi un valido fondamento giuridico per i trasferimenti internazionali di dati verso paesi terzi e organizzazioni internazionali ai sensi dell'articolo 49, paragrafo 1, lettera a), ed è su tali elementi che verte questo documento.

Pertanto la sezione 1 delle presenti linee guida è da considerarsi in combinato disposto con le linee guida sul consenso del gruppo di lavoro "Articolo 29", approvate dal comitato europeo per la protezione dei dati, che forniscono un'analisi più dettagliata dell'interpretazione delle condizioni generali e dei criteri per il consenso previsti dal RGPD[13]. Va altresì rilevato che, in virtù dell'articolo 49, paragrafo 3, le autorità pubbliche nell'esercizio dei pubblici poteri non possono ricorrere a questa deroga.

In virtù dell'articolo 49, paragrafo 1, lettera a), il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso in mancanza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, o di garanzie adeguate ai sensi dell'articolo 46, comprese le norme vincolanti d'impresa, purché "*l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate*".

2.1.1 IL CONSENSO DEVE ESSERE ESPLICITO

Ai sensi dell'articolo 4, paragrafo 11, del RGPD, il consenso deve essere una manifestazione di volontà libera, specifica, informata e inequivocabile. Su quest'ultima condizione l'articolo 49, paragrafo 1, lettera a), è più restrittivo, in quanto richiede un consenso "esplicito". Trattasi di un requisito nuovo anche rispetto all'articolo 26, paragrafo 1, lettera a), della direttiva 95/46/CE, che prevedeva soltanto un consenso "inequivocabile". Il RGPD richiede un consenso esplicito laddove possano presentarsi dei rischi per la protezione dei dati e, pertanto, si rende necessario un elevato livello di controllo individuale dei dati personali, come nel caso del trattamento di categorie particolari di dati (articolo 9, paragrafo 2, lettera a)) e delle decisioni automatizzate (articolo 22, paragrafo 2, lettera c)). Tali rischi particolari si presentano anche nell'ambito dei trasferimenti internazionali di dati.
Per ulteriori indicazioni sul requisito del consenso esplicito, e per gli altri requisiti applicabili ai fini della validità del consenso, si rimanda alle linee guida sul consenso del gruppo di lavoro "Articolo 29", approvate dal comitato europeo per la protezione dei dati[14].

2.1.2 IL CONSENSO DEVE ESSERE SPECIFICO PER IL TRASFERIMENTO O I TRASFERIMENTI DI DATI IN QUESTIONE

Tra i requisiti per la validità del consenso vi è la specificità. Perché possa essere un fondamento valido per il trasferimento dei dati ai sensi dell'articolo 49, paragrafo 1, lettera a), il consenso deve essere prestato in modo specifico per il trasferimento o per i trasferimenti di dati in questione.

L'elemento di "specificità" presente nella definizione del consenso intende garantire un certo grado di controllo da parte dell'utente e di trasparenza per l'interessato. Tale elemento è strettamente correlato al requisito del consenso "informato".

Poiché il consenso deve essere specifico, talvolta non è possibile ottenerlo in via preventiva per un trasferimento futuro già all'atto della raccolta dei dati; se ad esempio le circostanze specifiche e il trasferimento stesso non sono noti al momento in cui è richiesto il consenso, non è possibile verificarne l'impatto sull'interessato. Si ponga il caso in cui un'azienda UE raccolga i dati dei propri clienti per una finalità specifica (consegna merci) senza prevedere, in quel momento, il trasferimento di tali dati a terzi al di fuori dell'Unione. Si ipotizzi che alcuni anni dopo l'azienda sia rilevata da una società di un paese terzo, che intende trasferire i dati personali dei clienti a un'altra azienda di un paese terzo. Perché il trasferimento sia valido in applicazione della deroga, l'interessato deve prestare il proprio consenso per quel trasferimento specifico al momento in cui si prospetta tale operazione. Il consenso fornito all'atto della raccolta dei dati da parte dell'azienda dell'Unione ai fini della consegna non è sufficiente a giustificare il ricorso a questa deroga ai fini di un trasferimento di dati personali al di fuori dell'UE prospettatosi in un secondo momento.

L'esportatore deve quindi assicurarsi di ricevere un consenso specifico prima di mettere in atto il trasferimento, anche se ciò avviene dopo la raccolta dei dati. Tale requisito è correlato alla necessità di un consenso informato. È possibile ottenere il consenso specifico dell'interessato prima del trasferimento e all'atto della raccolta dei dati personali purché l'interessato sia informato del trasferimento specifico e le circostanze del trasferimento non siano modificate dopo la prestazione del consenso specifico da parte dell'interessato. L'esportatore dei dati deve accertarsi anche dell'osservanza dei requisiti esposti di seguito nella sezione 1.3.

2.1.3 IL CONSENSO DEVE ESSERE INFORMATO[15], SOPRATTUTTO RISPETTO AI POSSIBILI RISCHI DEL TRASFERIMENTO

Tale condizione è di estrema importanza in quanto rafforza e specifica ulteriormente il requisito generale del consenso "informato", applicabile a qualunque consenso e riportato all'articolo 4, paragrafo 11[16]. Il requisito generale del consenso "informato", di per sé, prevede che, nel caso del consenso quale fondamento di liceità per un trasferimento di dati ai sensi dell'articolo 6, paragrafo 1, lettera a), l'interessato sia preventivamente e adeguatamente informato delle circostanze specifiche del trasferimento (ossia l'identità del titolare del trattamento, la finalità del trasferimento, la tipologia dei dati da trasferire, l'esistenza del diritto di revoca del consenso, l'identità o le categorie dei destinatari)[17].

Oltre al requisito generale del consenso "informato", laddove siano trasferiti dati personali verso paesi terzi ai sensi dell'articolo 49, paragrafo 1, lettera a), questa disposizione prevede che l'interessato sia informato anche dei rischi specifici derivanti dal trasferimento verso un paese terzo che non offre una protezione adeguata e della mancata attuazione di adeguate garanzie per la protezione dei dati. La trasmissione di tali informazioni è fondamentale affinché l'interessato possa acconsentire nella piena consapevolezza di tali aspetti specifici del trasferimento e pertanto, qualora tali informazioni non siano condivise, la deroga non è applicabile.

Le informazioni fornite all'interessato per ottenere il consenso al trasferimento di dati personali a terzi con sede in paesi terzi devono specificare inoltre tutti i destinatari o tutte le categorie di destinatari dei dati e tutti i paesi verso i quali sono trasferiti i dati; devono riportare che il consenso rappresenta il fondamento giuridico per il trasferimento e che il paese terzo verso cui saranno trasferiti i dati non offre un livello adeguato di protezione dei dati sulla base di una decisione della Commissione europea[18]. Inoltre, come menzionato in precedenza, occorre fornire informazioni sui possibili rischi per l'interessato derivanti dalla mancanza di un'adeguata protezione nel paese terzo e dall'assenza di garanzie appropriate. Tale avviso, che potrebbe essere standardizzato, deve includere ad esempio una menzione della possibile assenza nel paese terzo di un'autorità di controllo e della possibilità che non siano previsti principi sul trattamento dei dati o diritti dell'interessato.

Nel caso specifico in cui un trasferimento avvenga dopo la raccolta di dati personali dall'interessato, l'esportatore è tenuto a informare l'interessato del trasferimento e dei rischi correlati prima che il trasferimento abbia luogo, così da ottenere il suo esplicito consenso al trasferimento "proposto".

Come dimostrato dall'analisi di cui sopra, il RGPD prevede soglie rigorose per il ricorso alla deroga del consenso. Tali restrizioni, in associazione alla possibilità per l'interessato di revocare il consenso in qualunque momento, fanno sì che il consenso possa rivelarsi una soluzione inapplicabile nel lungo periodo per i trasferimenti verso paesi terzi.

2.2 IL TRASFERIMENTO È NECESSARIO ALL'ESECUZIONE DI UN CONTRATTO CONCLUSO TRA L'INTERESSATO E IL TITOLARE DEL TRATTAMENTO OVVERO ALL'ESECUZIONE DI MISURE PRECONTRATTUALI ADOTTATE SU ISTANZA DELL'INTERESSATO - ARTICOLO 49, PARAGRAFO 1, LETTERA B)

Ai sensi del considerando 111, i trasferimenti di dati basati su questa deroga sono ammessi "se il trasferimento è ***occasionale*** e ***necessario*** in relazione a un contratto (...)."[19]

In generale, sebbene possa sembrare che le deroghe legate all'esecuzione siano potenzialmente piuttosto ampie, il loro campo di applicazione è limitato dai criteri di "*necessità*" e di "*occasionalità*" dei trasferimenti.

Necessità del trasferimento di dati

Il "*test di necessità*"[20] limita i casi in cui è possibile ricorrere all'articolo 49, paragrafo 1, lettera b)[21] e richiede un nesso stretto e significativo fra il trasferimento dei dati e la finalità del contratto.

Il ricorso a questa deroga non è ammesso ad esempio qualora un gruppo societario abbia centralizzato per finalità aziendali la gestione delle risorse umane e i pagamenti per tutto il personale in un paese terzo, poiché non vi è alcun nesso diretto e oggettivo tra l'esecuzione del contratto di lavoro e il trasferimento dei dati[22]. Altri presupposti per il trasferimento di cui al Capo V, quali clausole contrattuali tipo o norme vincolanti d'impresa, possono tuttavia risultare appropriati nel caso di specie.

Per contro, nel caso delle agenzie di viaggio il trasferimento di dati personali di singoli clienti verso strutture ricettive o altri partner commerciali coinvolti nell'organizzazione del soggiorno all'estero del cliente può essere reputato necessario per la finalità del contratto sottoscritto dall'agente e dal cliente, poiché vi è un nesso sufficientemente stretto e significativo tra il trasferimento dei dati e le finalità del contratto (organizzazione del viaggio del cliente).

Questa deroga non può essere applicata ai trasferimenti di informazioni aggiuntive non necessarie per l'esecuzione del contratto o, rispettivamente, di misure precontrattuali richieste dall'interessato[23]; per i dati aggiuntivi sono richiesti pertanto altri strumenti.

Trasferimenti occasionali

Questa deroga ammette il trasferimento di dati personali soltanto nel caso di un trasferimento occasionale[24]. Il carattere "*occasionale*" o "*non occasionale*" del trasferimento o dei trasferimenti deve essere valutato caso per caso.

Un trasferimento può considerarsi occasionale, ad esempio, qualora i dati personali di un responsabile delle vendite, che per contratto si reca presso vari clienti in paesi terzi, debbano essere inviati ai clienti per l'organizzazione delle riunioni. Un altro esempio di trasferimento occasionale potrebbe riguardare un istituto di credito dell'Unione europea che trasferisca dati personali a un altro istituto di un paese terzo per effettuare un pagamento per conto di un cliente, purché il trasferimento non avvenga nell'ambito di un rapporto di cooperazione stabile tra i due istituti.

Per contro, nel caso in cui una multinazionale organizzi corsi di formazione presso un centro in un paese terzo e trasferisca sistematicamente i dati personali dei dipendenti che partecipano al corso (ad esempio nome e qualifica professionale, ma potenzialmente anche esigenze alimentari o limitazioni di mobilità) i trasferimenti non possono definirsi "occasionali". I trasferimenti di dati effettuati con regolarità nell'ambito di un rapporto stabile sarebbero considerati sistematici e ripetuti e, pertanto, privi del carattere "occasionale". In tal caso molti trasferimenti di dati nell'ambito di un rapporto commerciale non possono pertanto fondarsi sull'articolo 49, paragrafo 1, lettera b).

In virtù dell'articolo 49, paragrafi 1 e 3, questa deroga non si applica alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri.

2.3 IL TRASFERIMENTO È NECESSARIO PER LA CONCLUSIONE O L'ESECUZIONE DI UN CONTRATTO STIPULATO TRA IL TITOLARE DEL TRATTAMENTO E UN'ALTRA PERSONA FISICA O GIURIDICA A FAVORE DELL'INTERESSATO - ARTICOLO 49, PARAGRAFO 1, LETTERA C)

L'interpretazione di questa disposizione è necessariamente analoga a quella dell'articolo 49, paragrafo 1, lettera b), pertanto il trasferimento di dati verso un paese terzo o un'organizzazione internazionale in mancanza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, o di garanzie adeguate ai sensi dell'articolo 46, può rientrare nella deroga di cui all'articolo 49, paragrafo 1, lettera c), qualora si possa considerare "*necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato*".

Oltre al requisito della necessità, ai sensi del considerando 111 i trasferimenti di dati possono avere luogo soltanto "*se il trasferimento* è ***occasionale*** *e* ***necessario*** *in relazione a un contratto (...)*". Pertanto, esulando dal "*test di necessità*", anche in questo caso i dati personali possono essere trasferiti in virtù di questa deroga soltanto se il trasferimento ha un carattere occasionale.

Necessità del trasferimento di dati e conclusione del contratto a favore dell'interessato

Qualora per motivi commerciali un'organizzazione avesse esternalizzato attività quali la gestione delle paghe al di fuori dell'Unione, questa deroga non giustifica trasferimenti di dati dettati da tali finalità, dal momento che non sussiste un nesso diretto e significativo fra il trasferimento dei dati e un contratto stipulato nell'interesse dell'interessato, anche se la finalità ultima del trasferimento è la gestione della retribuzione del dipendente[25]. Per tali trasferimenti possono risultare più appropriati altri strumenti di cui al Capo V, quali clausole contrattuali tipo o norme vincolanti d'impresa.

Trasferimenti occasionali

I dati personali possono essere trasferiti in applicazione di questa deroga allorché il trasferimento sia occasionale, come previsto all'articolo 49, paragrafo 1, lettera b). Pertanto, al fine di valutare il carattere occasionale del trasferimento, occorre applicare il medesimo test[26].

Da ultimo, in virtù dell'articolo 49, paragrafi 1 e 3, questa deroga non si applica alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri[27].

2.4 IL TRASFERIMENTO È NECESSARIO PER IMPORTANTI MOTIVI DI INTERESSE PUBBLICO - ARTICOLO 49, PARAGRAFO 1, LETTERA D)

Questa deroga, generalmente indicata come "deroga per importanti motivi di interesse pubblico", è molto simile alla disposizione di cui all'articolo 26, paragrafo 1, lettera d), della direttiva 95/46/CE[28], in base alla quale il trasferimento può avvenire soltanto qualora sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante.

In virtù dell'articolo 49, paragrafo 4, questa deroga si applica soltanto in presenza di un interesse pubblico riconosciuto dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento.

Tuttavia per l'applicazione della deroga non è sufficiente che il trasferimento di dati sia richiesto (ad esempio da un'autorità di un paese terzo) per un'indagine dettata da un interesse pubblico di un paese terzo che, in senso astratto, esiste anche nel diritto dell'Unione o dello Stato membro. Qualora per esempio un'autorità di un paese terzo richieda un trasferimento di dati per un'indagine mirata alla lotta al terrorismo, la mera esistenza di una normativa dell'Unione o dello Stato membro per la lotta al terrorismo non costituisce un elemento

sufficiente all'applicazione dell'articolo 49, paragrafo 1, lettera d), al trasferimento in oggetto. Piuttosto, come già sottolineato in altri frangenti[29] dal gruppo di lavoro "Articolo 29", predecessore del comitato europeo per la protezione dei dati, la deroga si applica soltanto quando dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento si possa dedurre, in aggiunta, che i trasferimenti in questione sono ammessi per rilevanti finalità di interesse pubblico, anche in virtù della reciprocità per la cooperazione internazionale. L'esistenza di un accordo o di una convenzione internazionale che stabilisca un determinato obiettivo, da favorire con la cooperazione internazionale, può essere un indicatore ai fini della valutazione dell'esistenza di un interesse pubblico ai sensi dell'articolo 49, paragrafo 1, lettera d), purché l'Unione europea o gli Stati membri abbiano sottoscritto tale accordo o convenzione.

Sebbene sia destinato principalmente all'utilizzo da parte delle autorità pubbliche, l'articolo 49, paragrafo 1, lettera d), può essere applicato anche da enti privati. Tale possibilità è comprovata da alcuni esempi riportati al considerando 112, che menziona trasferimenti da parte di autorità pubbliche ed enti privati[30].

Il requisito essenziale per l'applicabilità di questa deroga risiede pertanto nell'indicazione di un motivo di interesse pubblico rilevante e non nella natura dell'organizzazione (pubblica, privata o internazionale) che trasferisce o riceve i dati.

I considerando 111 e 112 indicano che la deroga non si limita ai trasferimenti di dati "occasionali"[31]. Ciò non significa tuttavia che, in base alla deroga per importanti motivi di interesse pubblico di cui all'articolo 49, paragrafo 1, lettera d), possano avere luogo trasferimenti di dati sistematici e su larga scala. Si richiede comunque l'osservanza del principio generale secondo cui le deroghe di cui all'articolo 49 non diverranno, nella pratica, la "regola" e la loro applicazione dovrà essere limitata a situazioni specifiche; ogni esportatore di dati dovrà inoltre garantire la conformità dei trasferimenti al rigido test di necessità[32].

Allorché i trasferimenti avvengano nell'ambito della normale attività o prassi commerciale il comitato europeo per la gestione dei dati raccomanda vivamente a tutti gli esportatori di dati (in particolare agli enti pubblici[33]) di mettere in atto adeguate garanzie ai sensi dell'articolo 46 invece di ricorrere alle deroghe di cui all'articolo 49, paragrafo 1, lettera d).

2.5 IL TRASFERIMENTO È NECESSARIO PER ACCERTARE, ESERCITARE O DIFENDERE UN DIRITTO IN SEDE GIUDIZIARIA - ARTICOLO 49, PARAGRAFO 1, LETTERA E)

Accertamento, esercizio o difesa di un diritto in sede giudiziaria

In virtù dell'articolo 49, paragrafo 1, lettera e), i trasferimenti sono ammessi

quando "*il trasferimento* è *necessario per accertare, esercitare o difendere un diritto in sede giudiziaria*". In base al considerando 111 il trasferimento può avvenire allorché sia "*occasionale e necessario in relazione a un contratto o un'azione legale, che sia in sede giudiziale, amministrativa o stragiudiziale, compresi i procedimenti dinanzi alle autorità di regolamentazione*". In tale clausola rientrano una serie di attività, ad esempio nell'ambito di un'indagine penale o amministrativa in un paese terzo (legge antitrust, corruzione, insider trading e situazioni simili), in cui la deroga può applicarsi a un trasferimento di dati a scopo di difesa oppure per ottenere un'esenzione oppure la riduzione di una sanzione prevista ai sensi di legge, ad esempio nelle indagini antitrust. Possono altresì rientrare nell'ambito di applicazione di questa deroga i trasferimenti di dati nelle procedure formali di produzione dei mezzi probatori in fase pre-processuale (*pre-trial discovery*), nonché azioni dell'esportatore di dati per l'istituzione di procedure in un paese terzo, ad esempio per l'apertura di un contenzioso o per la richiesta di approvazione di una fusione. Non è ammesso il ricorso alla deroga per giustificare il trasferimento di dati personali sulla base della mera possibilità di eventuali procedimenti giudiziari o procedure formali in futuro.

In virtù dell'articolo 49, paragrafo 3, la deroga non si applica alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri.

La combinazione delle espressioni "azioni legali" e "procedimenti" implica che i procedimenti in questione devono avere un fondamento giuridico, incluso un processo formale e giuridicamente definito, ma non si limita esclusivamente alle procedure giudiziarie o amministrative ("in sede [...] stragiudiziale"). Poiché il trasferimento deve essere effettuato **nell'ambito** del procedimento, è necessario un nesso stretto tra il trasferimento di dati e il procedimento specifico relativo alla situazione in questione. L'applicabilità astratta di un determinato tipo di procedimento non sarebbe sufficiente.

I titolari e i responsabili del trattamento devono essere consapevoli dell'eventuale presenza nel diritto nazionale dei cosiddetti "blocking statutes", che impediscono o limitano il trasferimento di dati personali verso autorità giudiziarie estere o talvolta organismi pubblici di altri paesi.

Necessità del trasferimento di dati

Un trasferimento di dati può avvenire soltanto se è **necessario** per accertare, esercitare o difendere un diritto. Questo "*test di necessità*" richiede un nesso stretto e significativo tra i dati in questione e lo specifico accertamento, esercizio o difesa di un diritto[34]. Il semplice interesse o la ricerca di un'eventuale maggiore "apertura" da parte delle autorità del paese terzo, di per sé, non sono sufficienti.

Sebbene un esportatore di dati possa essere tentato di trasferire tutti i dati personali potenzialmente rilevanti a fronte di una richiesta o per l'avvio di un'a-

zione legale, tale condotta non sarebbe conforme a questa deroga né al RGPD in generale in quanto il regolamento, in base al principio della minimizzazione dei dati, sottolinea come i dati personali debbano essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento.

Nell'ottica delle procedure di contenzioso, il gruppo di lavoro "Articolo 29", predecessore del comitato europeo per la protezione dei dati, ha già predisposto un approccio a più livelli che applica anche questo principio e consente di stabilire se i dati personali possano essere trasferiti. Quale primo passo occorre valutare con attenzione se, nel caso di specie, possano essere sufficienti dei dati anonimizzati. In alternativa si può considerare il trasferimento con l'uso di dati pseudonimizzati. Se invece fosse necessario inviare dati personali verso un paese terzo, prima del trasferimento bisogna valutare la pertinenza di tali informazioni nel contesto specifico, affinché siano trasferiti e comunicati soltanto i dati personali effettivamente necessari.

Trasferimento occasionale

I trasferimenti dovrebbero essere effettuati solo se presentano un carattere occasionale. Per ulteriori informazioni sulla definizione di trasferimento occasionale si rimanda alla sezione dedicata ai "trasferimenti occasionali e non ripetitivi"[35]. Gli esportatori di dati dovranno valutare con attenzione ogni singolo caso.

2.6 IL TRASFERIMENTO È NECESSARIO PER TUTELARE GLI INTERESSI VITALI DELL'INTERESSATO O DI ALTRE PERSONE, QUALORA L'INTERESSATO SI TROVI NELL'INCAPACITÀ FISICA O GIURIDICA DI PRESTARE IL PROPRIO CONSENSO - ARTICOLO 49, PARAGRAFO 1, LETTERA F)

La deroga di cui all'articolo 49, paragrafo 1, lettera f), si applica ovviamente al trasferimento di dati in caso di un'emergenza medica e allorché il trasferimento sia ritenuto direttamente necessario per la prestazione dei trattamenti sanitari previsti.

Pertanto, ad esempio, deve essere giuridicamente ammesso il trasferimento di dati (inclusi determinati dati personali) qualora il soggetto si trovi al di fuori dell'UE, in stato di incoscienza e necessiti di un'assistenza sanitaria urgente, e tali dati possano essere forniti soltanto da un esportatore (ad esempio il medico curante) con sede in uno Stato membro. In tali casi il diritto presuppone che il grave rischio imminente per la salute dell'interessato sia più rilevante delle preoccupazioni connesse alla protezione dei dati.

Il trasferimento deve essere correlato all'interesse individuale dell'interessato o di un'altra persona e, nel caso dei dati sanitari, deve essere necessario ai fini

di una diagnosi essenziale. Ne consegue che non si può ricorrere alla deroga per giustificare il trasferimento di dati personali relativi alla salute verso paesi esterni all'UE se la finalità del trasferimento non è una prestazione sanitaria espressamente rivolta all'interessato o a un'altra persona, bensì una ricerca medica generica che produrrà dei risultati soltanto in futuro.

Il RGPD non limita il ricorso alla deroga alla tutela dell'integrità fisica della persona e lascia spazio, ad esempio, alla valutazione di casi in cui si debba tutelare l'integrità mentale del soggetto. In tal caso l'interessato sarebbe peraltro incapace, a livello fisico o giuridico, di prestare il consenso per il trasferimento dei propri dati personali. L'interessato i cui dati personali sono oggetto del trasferimento deve inoltre trovarsi, per motivi fisici o giuridici, nell'impossibilità di prestare il proprio consenso al trasferimento in questione.

Allorché possieda la capacità decisionale e sia possibile chiedere il suo consenso, la deroga non è applicabile.

La richiesta di dati personali per evitare uno sfratto, ad esempio, non rientra nell'ambito di applicazione di questa deroga perché, sebbene una sistemazione abitativa possa considerarsi un interesse vitale, l'interessato può prestare il consenso al trasferimento dei propri dati.

La facoltà decisionale può essere compromessa da un'incapacità fisica, mentale o anche giuridica. Fatti salvi i sistemi di rappresentazione nazionali, l'incapacità giuridica riguarda ad esempio anche il caso di un minore. Tale incapacità deve essere dimostrata, a seconda dei casi, attraverso un certificato medico che attesti l'incapacità mentale dell'interessato oppure un documento ufficiale che ne riporti la condizione giuridica.

I trasferimenti di dati a un'organizzazione internazionale umanitaria, necessari per l'esecuzione di un compito derivante dalle convenzioni di Ginevra o al fine di rispettare il diritto internazionale umanitario applicabile nei conflitti armati, possono anch'essi rientrare nel disposto dell'articolo 49, paragrafo 1, lettera f) (cfr. considerando 112). Anche in questo caso l'interessato deve trovarsi nell'incapacità fisica o giuridica di prestare il proprio consenso.

Il trasferimento di dati a fronte di calamità naturali e per la condivisione di informazioni personali con enti e persone ai fini di operazioni di salvataggio e recupero (ad esempio parenti di vittime di calamità naturali oppure tramite servizi di emergenza e governativi) possono essere giustificati nell'ambito di questa deroga. Simili eventi imprevisti (quali alluvioni, terremoti o uragani) possono costituire una valida giustificazione al trasferimento urgente di determinati dati personali che consentano di individuare, ad esempio, la posizione e la condizione delle vittime. In tali circostanze si reputa che l'interessato sia impossibilitato a prestare il proprio consenso al trasferimento dei dati.

2.7 TRASFERIMENTO DA UN REGISTRO PUBBLICO - ARTICOLO 49, PARAGRAFO 1, LETTERA G) E ARTICOLO 49, PARAGRAFO 2

L'articolo 49, paragrafo 1, lettera g), e l'articolo 49, paragrafo 2, ammettono il trasferimento di dati personali contenuti nei registri in presenza di determinate condizioni. In generale per registro si intende un *documento (scritto) in cui sono annotati con regolarità determinati elementi o particolari* oppure *un elenco ufficiale riportante una serie di nomi o elementi*[36], tuttavia nell'accezione di cui all'articolo 49 il registro potrebbe essere in formato cartaceo o elettronico.

A norma del diritto dell'Unione o degli Stati membri, la finalità del registro in questione deve essere la trasmissione di informazioni al pubblico. I registri privati (a cura di enti privati) sono pertanto esclusi dall'ambito di applicazione di questa deroga (ad esempio i registri privati con cui si valuta l'affidabilità creditizia).

Il registro deve poter essere consultato:

a) dal pubblico in generale oppure
b) da chiunque sia in grado di dimostrare un legittimo interesse.

Trattasi, ad esempio, di: registri delle imprese, registri di associazioni, registri di condanne penali (registro del casellario giudiziale), registri catastali o pubblici registri automobilistici.

Oltre ai requisiti generali sulla compilazione dei registri stessi, i trasferimenti da tali registri sono ammessi soltanto se e nella misura in cui, per ciascun caso specifico, sono soddisfatti i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri (per le condizioni generali si veda l'articolo 49, paragrafo 1, lettera g)).

I titolari e i responsabili del trattamento che intendano fare ricorso a questa deroga per il trasferimento di dati personali devono essere consapevoli che il trasferimento non può riguardare la totalità dei dati personali o intere categorie di dati personali contenute nel registro (articolo 49, paragrafo 2). Allorché i dati siano trasferiti da un registro stabilito per legge e destinato a essere consultato da persone aventi un legittimo interesse, il trasferimento può avere luogo soltanto se tali persone lo richiedono o ne sono destinatarie, tenendo pienamente conto degli interessi e dei diritti fondamentali dell'interessato[37]. Nel valutare caso per caso l'adeguatezza del trasferimento, gli esportatori di dati dovranno sempre considerare gli interessi e i diritti dell'interessato.

Un ulteriore utilizzo dei dati personali contenuti nei registri di cui sopra è ammesso soltanto nel rispetto della legislazione applicabile in materia di protezione dei dati.

La deroga si applica anche alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri (articolo 49, paragrafo 3).

2.8 INTERESSI LEGITTIMI COGENTI - ARTICOLO 49, PARAGRAFO 1, COMMA 2

L'articolo 49, paragrafo 1, comma 2, introduce una nuova deroga che non era prevista dalla direttiva. In presenza di una serie di condizioni espressamente citate è ammesso il trasferimento di dati personali qualora sia necessario per il perseguimento degli interessi legittimi cogenti dell'esportatore dei dati.

Tale deroga è da prevista dalla normativa quale *extrema ratio* ed è applicabile soltanto "*se non* è *possibile basare il trasferimento su una disposizione dell'articolo 45 o 46, comprese le disposizioni sulle norme vincolanti d'impresa, e nessuna delle deroghe in specifiche situazioni* è *applicabile*".[38]

Questo approccio a più livelli alla valutazione del ricorso alle deroghe quale fondamento per i trasferimenti richiede di ponderare il possibile ricorso a uno strumento per il trasferimento di cui agli articoli 45 o 46 oppure a una delle deroghe specifiche descritte all'articolo 49, paragrafo 1, comma 1, prima di ricorrere alla deroga di cui all'articolo 49, paragrafo 1, comma 2. Il ricorso a questa deroga è ammesso soltanto nei casi residui ai sensi del considerando 113 ed è subordinato a un considerevole numero di condizioni espressamente elencate dalla legge. In linea con il principio di responsabilità sancito nel RGPD[39], l'esportatore di dati deve pertanto essere in grado di dimostrare che non sia stato possibile tutelare il trasferimento con garanzie adeguate ai sensi dell'articolo 46 né applicare una delle deroghe di cui all'articolo 49, paragrafo 1, comma 1.

Ciò significa che l'esportatore di dati è in grado di dimostrare seri tentativi in tal senso, tenuto conto delle circostanze del trasferimento. A seconda dei casi, per esempio, può trattarsi della dimostrazione di una verifica della possibilità di effettuare il trasferimento dei dati previo consenso esplicito al trasferimento da parte dell'interessato a norma dell'articolo 49, paragrafo 1, lettera a). In alcune situazioni tuttavia il ricorso ad altri strumenti nella pratica potrebbe risultare impossibile. Alcuni tipi di garanzie adeguate di cui all'articolo 46, per esempio, potrebbero essere un'opzione non realistica se l'esportatore di dati è una piccola o media impresa[40]. Il medesimo problema si presenta, ad esempio, allorché l'importatore di dati abbia espressamente rifiutato di sottoscrivere un contratto per il trasferimento dei dati in base alle clausole tipo di protezione dei dati (articolo 46, paragrafo 2, lettera c)) e non vi siano altre opzioni possibili (inclusa, a seconda dei casi, la scelta di un altro "importatore dei dati") - si veda anche il paragrafo seguente sugli interessi legittimi "cogenti".

Interessi legittimi cogenti del titolare del trattamento

In base alla formulazione della deroga, il trasferimento deve essere necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato. Una valutazione degli interessi dell'esportatore dei dati in qualità di responsabile del trattamento oppure dell'importatore dei dati non è rilevante.

Si osserva inoltre che soltanto gli interessi ritenuti "cogenti" sono rilevanti e tale precisazione riduce notevolmente l'ambito di applicazione della deroga, poiché non vi rientrano tutti i possibili "interessi legittimi" di cui all'articolo 6, paragrafo 1, lettera f). La restrizione risulta più incisiva, poiché gli interessi legittimi cogenti devono essere essenziali per il titolare del trattamento. Si consideri, ad esempio, il caso in cui il titolare del trattamento debba trasferire dati personali per proteggere la propria organizzazione o i relativi sistemi da un danno grave e immediato, oppure evitare una pesante sanzione che avrebbe forti ripercussioni sull'attività.

Trasferimento non ripetitivo

L'articolo 49, paragrafo 1, comma 2, specifica espressamente che le disposizioni in esso contenute si applicano soltanto a trasferimenti non ripetitivi[41].

Numero limitato di interessati

Il trasferimento deve riguardare inoltre un numero limitato di interessati. La soglia massima non è stata definita in termini assoluti in quanto dipende dal contesto ma, tenuto conto del tipo di trasferimento, il numero degli interessati deve essere adeguatamente contenuto.

Nella pratica, il concetto di "numero limitato di interessati" varia in base ai singoli casi. Qualora ad esempio il titolare del trattamento si trovi nella condizione di dover trasferire dati personali per individuare un grave e anomalo incidente relativo alla sicurezza al fine di proteggere la propria organizzazione, si dovrà valutare quanti dati dei dipendenti è necessario trasferire per il conseguimento di questo interesse legittimo cogente.

Pertanto, per poter applicare la deroga, il trasferimento non dovrà riguardare tutto il personale del titolare del trattamento ma soltanto un piccolo gruppo di dipendenti.

Bilanciare gli "interessi legittimi cogenti del titolare del trattamento" e gli "interessi o i diritti e le libertà dell'interessato" in base a una valutazione di tutte le circostanze relative al trasferimento e fornendo garanzie adeguate

Un ulteriore requisito consiste nello svolgimento di un test comparativo che valuti l'interesse legittimo (cogente) perseguito dell'esportatore rispetto agli interessi o i diritti e le libertà dell'interessato. In proposito la legge chiede espressamente all'esportatore di valutare tutte le circostanze relative al trasferimento in oggetto e, in base a tale valutazione, di offrire "garanzie adeguate" per la protezione dei dati trasferiti. Tale requisito sottolinea il ruolo speciale che possono svolgere le garanzie nella riduzione dell'indebito impatto sugli in-

teressati, modificando in tal modo l'equilibrio tra i diritti e gli interessi in misura tale che l'interesse legittimo degli interessati non prevalga sull'interesse legittimo del responsabile del trattamento dei dati[42].

Quanto agli interessi, ai diritti e alle libertà dell'interessato da tenere in considerazione, i possibili effetti negativi, ossia i rischi del trasferimento per qualunque tipo di interesse (legittimo) dell'interessato, devono essere attentamente previsti e valutati tenendone presente il livello di probabilità e gravità[43]. A tale proposito occorre tenere presente qualunque possibile danno (fisico e materiale ma anche immateriale, ad esempio relativo a un pregiudizio della reputazione)[44]. Nel valutare tali rischi e le garanzie che, nelle circostanze specifiche, si possono reputare "adeguate" per i diritti e le libertà dell'interessato, l'esportatore dei dati deve prestare particolare attenzione alla natura dei dati, alla finalità e alla durata del trattamento nonché alla situazione del paese d'origine, del paese terzo e, se del caso, del paese di destinazione finale del trasferimento[45].

La legge richiede inoltre all'esportatore l'applicazione di misure supplementari quale garanzia per ridurre al minimo i rischi individuati per l'interessato a fronte del trasferimento[46]. Tale requisito è obbligatorio ai sensi di legge pertanto, in assenza di garanzie supplementari, sugli interessi al trasferimento del titolare del trattamento prevarranno in ogni caso gli interessi o i diritti e le libertà dell'interessato[47]. Quanto alla natura di tali garanzie, non è possibile stabilire requisiti generali applicabili a qualunque trasferimento poiché le garanzie variano in base ai singoli casi. A seconda delle circostanze le garanzie potranno includere, per esempio, misure volte a garantire la cancellazione dei dati appena possibile dopo il trasferimento oppure a limitare le finalità per le quali i dati possano essere trattati dopo il trasferimento. Un'attenzione particolare dovrebbe essere prestata alla possibilità di trasferire soltanto dati cifrati o pseudonimizzati[48]. Si dovrebbero considerare inoltre misure tecniche e organizzative volte a garantire che i dati trasferiti non possano essere utilizzati per finalità diverse da quelle strettamente previste dall'esportatore.

Informazione dell'autorità di controllo

L'obbligo di informare l'autorità di controllo non implica l'autorizzazione al trasferimento da parte di quest'ultima ma costituisce piuttosto un'ulteriore garanzia, in quanto consente all'autorità di controllo (qualora lo reputi opportuno) di valutare il trasferimento dei dati rispetto al possibile impatto sui diritti e sulle libertà degli interessati. Ai fini della conformità al principio di responsabilità, si raccomanda all'esportatore di dati di registrare tutti gli aspetti rilevanti del trasferimento, quali l'interesse legittimo cogente perseguito, gli interessi "concorrenti" della persona, la natura dei dati trasferiti e la finalità del trasferimento.

Notificare all'interessato il trasferimento e gli interessi legittimi cogenti perseguiti

Il responsabile del trattamento è tenuto a informare l'interessato del trasferimento e degli interessi legittimi cogenti perseguiti. Tali informazioni devono essere fornite in aggiunta a quelle richieste ai sensi degli articoli 13 e 14 del RGPD.

Per il comitato europeo
per la protezione dei dati
Il presidente

(Andrea Jelinek)

NOTE

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[2] Gruppo di lavoro "Articolo 29", "Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE, del 24 ottobre 1995", 25 novembre 2005 (WP 114).

[3] Gruppo di lavoro "Articolo 29", WP 114, pag. 10, e gruppo di lavoro "Articolo 29", Documento di lavoro sulla sorveglianza delle comunicazioni elettroniche per i servizi di intelligence di sicurezza nazionale (WP 228), pag. 39.

[4] Gruppo di lavoro "Articolo 29", WP 114, pag. 9.

[5] Considerando 114.

[6] Gruppo di lavoro "Articolo 29", WP 114, pag. 8.

[7] Come sopra, gruppo di lavoro "Articolo 29", WP 114, pag. 8. La Corte di giustizia dell'Unione europea ha ripetutamente sottolineato che "la tutela del diritto fondamentale al rispetto della vita privata a livello dell'Unione esige che le deroghe e le restrizioni alla tutela dei dati personali intervengano entro i limiti dello stretto necessario" (sentenze del 16 dicembre 2008, Satakunnan Markkinapörssi e Satamedia, C 73/07, punto 56; del 9 novembre 2010, Volker und Markus Schecke e Eifert, C 92/09 e C 93/09, punto 77; Digital Rights, punto 52; del 6 ottobre 2015, Schrems, C 362/14, punto 92, nonché del 21 dicembre 2016, Tele2 Sverige AB, C 203/15, punto 96). Si veda anche la relazione sul protocollo addizionale alla Convenzione 108 sulle autorità di controllo e sui flussi di dati transfrontalieri, articolo 2, paragrafo 2, lettera a), pag. 6, accessibile dal sito https://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/181.1).

[8] NDR. Questa nota è stata erroneamente inserita nella versione ufficiale delle linee guida ed è qui riportata solo per mantenere la coerenza nei riferimenti del testo.

[9] Cfr. considerando 115, quarto periodo.

[10] Ai sensi dell'articolo 4, paragrafo 11, del RGPD, per "consenso dell'interessato" si intende qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

[11] Anche i considerando 32, 33, 42 e 43 forniscono ulteriori orientamenti sul consenso.

[12] Cfr. Linee guida sul consenso ai sensi del regolamento (UE) 2016/679 (WP 259), del gruppo di lavoro "Articolo 29".

[13] Idem.

[14] Idem.

[15] È richiesta inoltre l'osservanza dei requisiti generali di trasparenza di cui agli articoli 13 e 14 del RGPD. Per ulteriori informazioni, consultare le linee guida sulla trasparenza ai sensi del regolamento 2016/679 (WP 260).

[16] Cfr. Linee guida sul consenso ai sensi del regolamento (UE) 2016/679 (WP 259), del gruppo di lavoro "Articolo 29".

[17] Idem, pagina 14.

[18] L'ultimo requisito citato deriva anche dal dovere di informare gli interessati, di cui all'articolo 13, paragrafo 1, lettera f), e all'articolo 14, paragrafo 1, lettera e).

[19] Il criterio del carattere "occasionale" dei trasferimenti si ritrova al considerando 111 e si applica alle deroghe di cui all'articolo 49, paragrafo 1, lettere b), c) ed e).

[20] Cfr. anche il parere 06/2014 del gruppo di lavoro "Articolo 29" sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE (WP 217).

[21] Il requisito della "necessità" ricorre anche nelle deroghe di cui all'articolo 49, paragrafo 1, dalla lettera c) alla lettera f).

[22] In tal caso inoltre il trasferimento non sarebbe reputato occasionale (si veda in appresso).

[23] Più in generale, tutte le deroghe di cui all'articolo 49, paragrafo 1, lettere da b) a f), consentono di trasferire soltanto i dati necessari per la finalità del trasferimento.

[24] Per una definizione generale del termine "occasionale" si rimanda a pagina 4.

[25] In tal caso inoltre il trasferimento non sarebbe reputato occasionale (si veda in appresso).

[26] Per una definizione generale del termine "occasionale" si rimanda a pagina 4.

[27] Per ulteriori informazioni si rimanda alla precedente sezione 1, pagina 5.

[28] DIRETTIVA 95/46/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

[29] Parere 10/2006 del gruppo di lavoro "Articolo 29" sul trattamento dei dati personali da parte della Società per le telecomunicazioni finanziarie interbancarie mondiali (SWIFT) (WP 128), pag. 28.

[30] "*Scambio internazionale di dati tra autorità garanti della concorrenza, amministrazioni fiscali o doganali, autorità di controllo finanziario, servizi competenti in materia di sicurezza sociale o sanità pubblica, ad esempio in caso di ricerca di contatti per malattie contagiose o al fine di ridurre e/o eliminare il doping nello sport.*"

[31] Per una definizione generale del termine "occasionale" si rimanda a pagina 4.

[32] Cfr. anche pag. 3.

[33] Ad esempio le autorità di controllo finanziario che scambiano dati nell'ambito dei trasferimenti internazionali di dati personali ai fini della cooperazione amministrativa.

[34] Considerando 111: "necessario in relazione a un contratto o un'azione legale".

[35] Pagina 4

[36] Merriam Webster Dictionary, https://www.merriam-webster.com/dictionary/register (22.01.2018); Oxford Dictionary https://en.oxforddictionaries.com/definition/register (22.01.2018).

[37] Considerando 111 del RGPD.

[38] Articolo 49, paragrafo 1, comma 2, del RGPD.

[39] Articolo 5, paragrafo 2, e articolo 24, paragrafo 1.

[40] Le norme vincolanti d'impresa, ad esempio, spesso possono essere un'opzione impraticabile per le piccole e medie imprese in considerazione degli onerosi investimenti amministrativi necessari.

[41] Per ulteriori informazioni sull'espressione "non ripetitivo", si veda pagina 4.

[42] L'importanza delle garanzie nell'equilibrio tra gli interessi del titolare del trattamento e quelli dell'interessato è già stato evidenziato dal gruppo di lavoro "Articolo 29" nel documento WP 217, pag. 36.

[43] Cfr. il considerando 75: "*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse (...)*".

[44] Cfr. il considerando 75: "*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale.*"

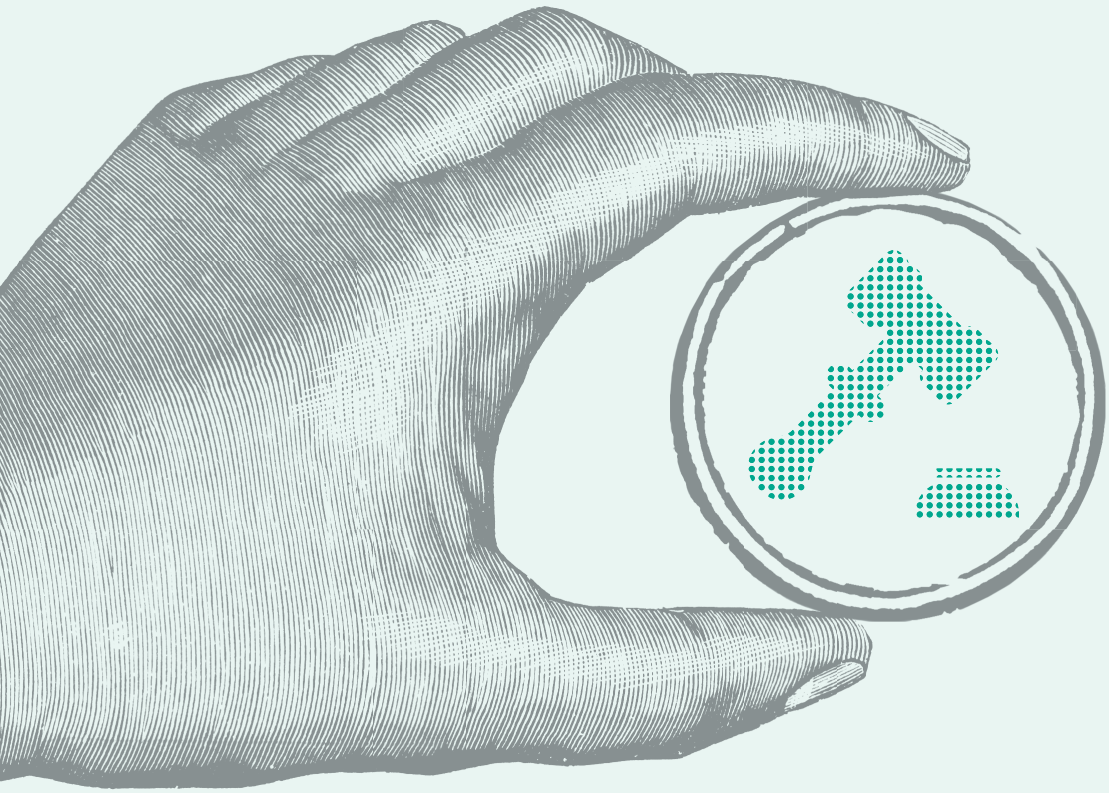
[45] Considerando 113.

[46] Nell'ambito del test comparativo "normale" previsto ai sensi di legge tali misure (aggiuntive) potrebbero non essere necessarie in tutti i casi (cfr. il documento di lavoro del gruppo di lavoro "Articolo 29" sul progetto delle clausole contrattuali ad hoc "da responsabile del trattamento dei dati dell'UE a ulteriore responsabile non UE" (documento WP 214, pag. 41), invece la formulazione dell'articolo 49, paragrafo 1, comma 2, lascia intendere il carattere obbligatorio delle misure aggiuntive affinché il trasferimento di dati sia conforme al test comparativo e sia pertanto ammesso con il ricorso a questa deroga.

[47] Nell'ambito del test comparativo "normale" previsto ai sensi di legge tali misure (aggiuntive) potrebbero non essere necessarie in tutti i casi (cfr. il parere 6/2014 del gruppo di lavoro "Articolo 29" sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE (documento WP 217, pag. 49), invece la formulazione dell'articolo 49, paragrafo 1, comma 2, lascia intendere il carattere obbligatorio delle misure aggiuntive affinché il trasferimento di dati sia conforme al test comparativo e sia pertanto ammesso con il ricorso a questa deroga.

[48] Per ulteriori esempi di possibili garanzie, si rimanda al documento di lavoro del gruppo di lavoro "Articolo 29" sul progetto delle clausole contrattuali ad hoc "da responsabile del trattamento dei dati dell'UE a ulteriore responsabile non UE" (WP 214), pagg. 41-43.

4 Meccanismi di applicazione del GDPR



Premessa
Meccanismi di applicazione del GDPR

Alcune delle novità più importanti del GDPR riguardano i meccanismi preposti alla sua applicazione da parte delle Autorità di controllo, come il Garante, incaricate di vigilarne l'osservanza.

Fra tali fondamentali innovazioni del GDPR vi è la previsione di un meccanismo di "sportello unico" per le imprese e le aziende che abbiano più stabilimenti nell'Ue nel contesto delle cui attività svolgano trattamenti di dati personali, o che offrano prodotti o servizi in più di un Paese dell'Ue a partire da un solo stabilimento in uno Stato membro. Lo sportello unico è l'Autorità di controllo dello Stato membro ove quel titolare o responsabile ha il proprio stabilimento unico o principale, e tale Autorità funge da interlocutore unico del titolare o del responsabile anche per tutti i reclami o i contenziosi che dovessero sorgere in altri Paesi dell'Ue. Questa Autorità è detta propriamente "Autorità capofila" e il WP29 ha precisato i criteri per la sua individuazione da parte del titolare o del responsabile, sulla base delle disposizioni del GDPR e dei principi generali che quest'ultimo ha confermato quanto al ruolo e alle caratteristiche del responsabile e del titolare di un trattamento. Alle linee-guida si associano FAQ che offrono un percorso guidato verso l'individuazione corretta dello sportello unico, nei casi ove ciò è contemplato.

Il GDPR ha attribuito a tutte le Autorità di controllo nazionali poteri correttivi molto ampi, fra cui il potere di irrogare sanzioni amministrative pecuniarie (ai sensi dell'Art. 83). Si tratta per alcuni Paesi Ue di una novità assoluta, poiché le Autorità di controllo di tali Paesi – a differenza di quanto vale per l'Italia - non disponevano di alcuna potestà sanzionatoria diretta prima dell'entrata in vigore del GDPR. Si è reso dunque necessario per il WP29 fornire alcune indicazioni interpretative delle disposizioni dell'Art. 83, che funge da lex specialis in merito all'irrogazione delle sanzioni pecuniarie e contiene un elenco di criteri di cui le Autorità devono tenere conto nel decidere se e in quale misura procedere nei confronti di un titolare che abbia violato una delle disposizioni del GDPR elencate all'Art. 83.

Linee guida per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento [WP 244 rev. 01]

Adottate il 13 dicembre 2016
Versione emendata e adottata in data aprile 2017

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della Commissione europea, direzione generale Giustizia e consumatori, B -1049 Bruxelles, Belgio, ufficio MO59 05/35.

Sito Internet: http://ec.europa.eu/justice/data-protection/index_en.htm

Indice

1. INDIVIDUAZIONE DELL'AUTORITÀ DI CONTROLLO CAPOFILA: FONDAMENTI CONCETTUALI

1.1 TRATTAMENTO TRANSFRONTALIERO DI DATI PERSONALI

L'esigenza di individuare l'autorità di controllo capofila sorge solo se il titolare del trattamento o responsabile del trattamento effettua un trattamento transfrontaliero di dati personali. In base all'articolo 4, punto 23, del regolamento generale sulla protezione dei dati (RGPD), per "trattamento transfrontaliero" si intende:

- *[il] trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure*

- *[il] trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.*

Ne deriva che una società con stabilimenti in Francia e Romania, per esempio, che tratta i dati personali nel contesto delle attività di tali stabilimenti effettua trattamenti transfrontalieri.

La stessa società potrebbe trattare i dati soltanto nel contesto dello stabilimento situato in Francia. Se però tale attività incide in modo sostanziale, o è probabile che incida in modo sostanziale, su interessati in Francia e in Romania, di nuovo saremo di fronte a un trattamento transfrontaliero.

1.1.1 "INCIDE IN MODO SOSTANZIALE"

Il RGPD non definisce né cosa si debba intendere per "in modo sostanziale" né il significato del verbo "incidere". Tale formulazione vuole garantire che nella definizione di "trattamento transfrontaliero" non rientri qualsiasi attività di trattamento, a prescindere dai suoi effetti, svolta nel contesto delle attività di un singolo stabilimento.

Il tenore letterale dell'aggettivo "sostanziale" (*substantial* nel testo inglese) viene esplorato nel testo originale con riguardo al lemma presente nell'*Oxford English Dictionary*. Per l'Italia, un approccio analogo postula di ricercare il lemma, per esempio, sul Dizionario Enciclopedico Treccani, dove si rinvengono le seguenti esemplificazioni: "che è relativo alla sostanza", "essenziale", "fondamentale", "di sostanza, di fondo", "con più diretta contrapposizione a ciò che è particolare o marginale"; ne vengono offerti come sinonimi "concreto, materiale, reale".

Lo stesso dicasi per il verbo "incidere" ([to] *affect* nel testo inglese). Nel Dizionario Treccani si rinvengono le seguenti esemplificazioni: "ricadere, gravare su qualcuno o qualche cosa", "influire profondamente, far risentire le conseguenze, lasciare profonda traccia su qualche cosa". Tutto ciò sembra indicare che un trattamento "incide" su qualcuno nella misura in cui ha un qualche tipo di impatto su tale soggetto. Un trattamento che non produce effetti sostanziali su una persona fisica non rientra nella seconda parte della definizione di "trattamento transfrontaliero"; tuttavia, a un trattamento del genere si applicherebbe la prima parte della definizione se esso avvenisse nel contesto delle attività di stabilimenti situati in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione, ove tale titolare o responsabile fosse stabilito in più di uno Stato membro.

Un trattamento è riconducibile alla parte b) della definizione di cui sopra se sussiste la probabilità di un suo effetto sostanziale, e non solo se si produce in concreto un effetto sostanziale. Si osservi che l'impiego dell'avverbio "probabilmente" esclude che si tratti di una possibilità remota: la probabilità del verificarsi di effetti sostanziali deve essere superiore alla probabilità che essi non si verifichino. D'altro canto, non è necessario che gli effetti su una persona fisica si producano in concreto: la probabilità di un effetto sostanziale è sufficiente a ricondurre il trattamento nell'ambito della definizione di "trattamento transfrontaliero".

La circostanza per cui un determinato trattamento comporta l'elaborazione di dati personali relativi a un numero anche elevato di persone fisiche in più Stati membri non implica necessariamente che tale trattamento produca effetti sostanziali, né che ciò sia probabile. Un trattamento che non produca effetti sostanziali non rappresenta un trattamento transfrontaliero ai fini della parte b) della relativa definizione, indipendentemente dal numero di persone sulle quali esso incide.

Nell'interpretare il senso dell'espressione "incide in modo sostanziale", le autorità di controllo valuteranno ciascun caso in rapporto alle specifiche circostanze, tenendo conto del contesto in cui si svolge il trattamento, del tipo di dati trattati, delle finalità del trattamento e di altri fattori fra cui in che misura il trattamento:

- sia causa, o probabile causa, di una perdita, un danno o un disagio per la persona;
- produca concretamente, o sia probabile che produca concretamente, una limitazione dei diritti o un'esclusione da benefici e opportunità;
- incida, o probabilmente incida, sulla salute, il benessere o la tranquillità della persona; o incida, o probabilmente incida, sulla situazione economica o finanziaria della persona; o esponga la persona a forme di discriminazione o disparità di trattamento;
- comporti l'analisi di categorie particolari di dati personali o di altri dati che configurano un'ingerenza nella sfera privata, in particolare dati personali di minori;

- sia causa, o probabile causa, di modifiche significative nella condotta della persona; o generi conseguenze impreviste, inattese o indesiderate per la persona;
- provochi situazioni di imbarazzo o altre conseguenze negative, compreso il danno reputazionale; ovvero
- comporti il trattamento di un'ampia gamma di dati personali.

Il criterio sintetizzato dalla formula "incide in modo sostanziale" è inteso a garantire, in ultima analisi, che le autorità di controllo siano tenute a cooperare secondo le procedure formalizzate nel meccanismo di coerenza del RGPD esclusivamente *"quando un'autorità di controllo intenda adottare una misura intesa a produrre effetti giuridici con riguardo ad attività di trattamento che incidono in modo sostanziale su un numero significativo di interessati in vari Stati membri"* (considerando 135).

1.2 AUTORITÀ DI CONTROLLO CAPOFILA

L' "autorità di controllo capofila" è sostanzialmente l'autorità cui spetta in prima battuta la gestione di un trattamento transfrontaliero – per esempio, in caso di reclami presentati da un interessato rispetto al trattamento dei suoi dati personali.

L'autorità di controllo capofila dovrà coordinare ogni attività di accertamento attraverso il coinvolgimento di altre autorità di controllo "interessate".

Per individuare l'autorità di controllo capofila occorre stabilire dove si trovi lo "stabilimento principale" ovvero lo "stabilimento unico" del titolare all'interno dell'UE. In base all'articolo 56 del RGPD:

- *l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60.*

1.3 STABILIMENTO PRINCIPALE

Ai sensi dell'articolo 4, punto 16, del RGPD, per "stabilimento principale" s'intende:

- *per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua* ***amministrazione centrale*** *nell'Unione, salvo che le* ***decisioni sulle finalità e i mezzi*** *del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia* ***facoltà di ordinare l'esecuzione di***

***tali decisioni**, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;*

- *con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento.*

2 PROCEDURA DI INDIVIDUAZIONE DELL'AUTORITÀ DI CONTROLLO CAPOFILA

2.1 INDIVIDUAZIONE DELLO "STABILIMENTO PRINCIPALE" DEL TITOLARE DEL TRATTAMENTO

Per stabilire dove si trovi lo stabilimento principale, occorre innanzitutto individuare il luogo dell'amministrazione centrale del titolare del trattamento nell'UE[1]. In base all'approccio sotteso al RGPD il luogo dell'amministrazione centrale nell'UE è quello in cui sono adottate le decisioni sulle finalità e i mezzi del trattamento di dati personali e che ha la facoltà di ordinare l'esecuzione di tali decisioni.

L'essenza del principio dell'autorità di controllo capofila previsto nel RGPD è che il controllo su un trattamento transfrontaliero sia svolto sotto la direzione di una sola autorità di controllo nell'UE. Qualora le decisioni su vari trattamenti transfrontalieri siano prese nel luogo dell'amministrazione centrale nell' UE, vi sarà un'unica autorità capofila per i diversi trattamenti transfrontalieri svolti dalla società multinazionale. Tuttavia, possono aversi casi in cui uno stabilimento diverso da quello ove ha sede l'amministrazione centrale assume decisioni autonome quanto alle finalità e ai mezzi di uno specifico trattamento. Ciò significa che, in determinate situazioni, potranno esservi più autorità capofila: è il caso, per esempio, di una multinazionale che decida di prevedere centri decisionali distinti, in distinti paesi, per distinti trattamenti.

Vale la pena di ricordare che se una società multinazionale centralizza tutte le decisioni relative alle finalità e ai mezzi dei rispettivi trattamenti presso uno dei suoi stabilimenti nell'UE (e se questo stabilimento dispone della facoltà di ordinare l'esecuzione di tali decisioni), allora vi sarà un'unica autorità di controllo capofila per la multinazionale in questione.

In casi del genere sarà fondamentale che la società definisca con precisione dove sono prese le decisioni sulle finalità e i mezzi del trattamento. Individuare correttamente lo stabilimento principale è nell'interesse del titolare del trattamento e del responsabile del trattamento perché elimina ogni ambiguità sull'autorità di controllo che fungerà da loro interlocutore per le varie incom-

benze previste dal regolamento: dalla designazione del responsabile della protezione dei dati (RPD), ove applicabile, alla consultazione dell'autorità in relazione a un trattamento a rischio che il titolare del trattamento non sia in grado di attenuare attraverso mezzi ragionevoli. Le disposizioni del regolamento in materia mirano a facilitare la gestione di queste incombenze.

Di seguito sono riportate alcune esemplificazioni:

Esempio 1: Una società alimentare ha la propria sede centrale (ossia il "luogo dell'amministrazione centrale") a Rotterdam, nei Paesi Bassi. La società possiede stabilimenti in altri paesi UE che si occupano dei contatti con gli interessati in tali paesi. Tutti gli stabilimenti utilizzano lo stesso software per trattare i dati personali dei consumatori a fini di marketing. Tutte le decisioni su finalità e mezzi del trattamento di dati per tali finalità sono assunte presso la sede centrale di Rotterdam. Ne deriva che l'autorità capofila per questi trattamenti transfrontalieri è l'autorità di controllo dei Paesi Bassi.

Esempio 2: La sede centrale di una banca si trova a Francoforte, e tutti[2] i trattamenti connessi all'attività bancaria sono gestiti da tale sede; tuttavia, l'ufficio assicurazioni della banca ha sede a Vienna. Se lo stabilimento situato a Vienna dispone dell'autorità per decidere su tutti i trattamenti connessi ad attività assicurative e ordinare l'esecuzione delle relative decisioni sull'intero territorio dell'UE, allora – come previsto dall'articolo 4, punto 16, del regolamento – sarà l'autorità di controllo austriaca a fungere da autorità capofila rispetto al trattamento transfrontaliero di dati personali per finalità assicurative, mentre le autorità tedesche (in questo caso, l'autorità di controllo del Land Assia) avranno il compito di monitorare il trattamento di dati personali per finalità bancarie ovunque si collochi la clientela[3].

2.1.1 CRITERI PER L'INDIVIDUAZIONE DELLO STABILIMENTO PRINCIPALE QUALORA ESSO NON CORRISPONDA AL LUOGO DELL'AMMINISTRAZIONE CENTRALE NELL'UE

Il considerando 36 fornisce utili chiarimenti sul criterio da usare in via primaria per definire quale sia lo stabilimento principale di un titolare del trattamento ove non trovi applicazione il criterio del luogo di amministrazione centrale. Si tratta di individuare dove si collochi l'esercizio reale ed effettivo delle attività gestionali tese a definire finalità e mezzi del trattamento nel quadro di un'organizzazione stabile. Il considerando 36 chiarisce, inoltre, che "la presenza o l'uso di mezzi tecnici e tecnologie di trattamento di dati personali o di attività di trattamento non costituiscono di per sé lo stabilimento principale né sono quindi criteri determinanti della sua esistenza".

Spetta al titolare del trattamento individuare dove si trovi il proprio stabilimento principale e, conseguentemente, quale sia l'autorità capofila; tuttavia, l'autorità di controllo volta per volta interessata può successivamente sollevare obiezioni rispetto a tale determinazione.

L'elenco riportato qui di seguito indica alcuni criteri utili per determinare la sede dello stabilimento principale del titolare del trattamento ai sensi del RGPD, qualora esso non costituisca il luogo dell'amministrazione centrale nell'UE.

- Dove viene dato il definitivo "via libera" alle decisioni su finalità e mezzi del trattamento? o Dove vengono prese le decisioni su attività societarie che comportano trattamenti di dati? o Dove si trova effettivamente la facoltà di ordinare l'esecuzione delle decisioni prese?
- Dove si trova l'amministratore (o gli amministratori) cui spetta la responsabilità gestionale complessiva del trattamento transfrontaliero?
- In quale paese risulta costituita la società titolare o responsabile del trattamento, se questa ha sede in un solo Stato?

Si osservi che l'elenco non è esaustivo; possono risultare pertinenti altri fattori in rapporto al singolo titolare del trattamento o al trattamento svolto. Se un'autorità di controllo ha motivo di dubitare della corretta identificazione dello stabilimento principale effettuata dal titolare del trattamento ai fini del RGPD, potrà sempre chiedere a tale titolare di fornirle le ulteriori informazioni necessarie a dimostrare dove si trovi effettivamente lo stabilimento principale.

2.1.2 GRUPPI IMPRENDITORIALI

Qualora un trattamento sia svolto da un gruppo imprenditoriale la cui sede centrale è situata nell'UE, si presume che lo stabilimento dell'impresa controllante sia il centro decisionale con riguardo al trattamento di dati personali e, quindi, rappresenti lo stabilimento principale del gruppo – tranne ove finalità e mezzi del trattamento siano decisi da un diverso stabilimento. È probabile che la sede operativa o controllante del gruppo sul territorio dell'UE sia lo stabilimento principale ai fini del regolamento, perché è in tale sede che si colloca il luogo dell'amministrazione centrale.

Nella definizione si fa riferimento al luogo dell'amministrazione centrale del titolare del trattamento, il che si attaglia perfettamente a quegli organismi che dispongono di una sede centrale, dove si trova il centro decisionale, e presentano una struttura ramificata. In casi del genere è evidente che la potestà decisionale sui trattamenti transfrontalieri e sull'esecuzione delle relative determinazioni spetta alla sede centrale, ed è quindi immediato definire la sede dello stabilimento principale e, conseguentemente, quale sia l'autorità di controllo capofila. Possono però esservi casi in cui il sistema decisionale di un gruppo imprenditoriale è più complesso e singoli stabilimenti dispongono di poteri decisionali indipendenti per quanto concerne i trattamenti transfrontalieri. I criteri sopra delineati possono aiutare i gruppi imprenditoriali nell'individuazione del rispettivo stabilimento principale.

2.1.3 CONTITOLARITÀ DEL TRATTAMENTO

Il regolamento non contiene indicazioni specifiche quanto all'individuazione dell'autorità capofila in presenza di due o più titolari del trattamento stabiliti nell'UE che definiscano congiuntamente finalità e mezzi del trattamento, ossia in situazioni di contitolarità del trattamento. L'articolo 26, paragrafo 1, e il considerando 79 chiariscono che i singoli contitolari devono stabilire, in modo trasparente, le rispettive responsabilità quanto all'osservanza degli obblighi che loro incombono in base al regolamento. Pertanto, al fine di beneficiare del principio dello "sportello unico", i contitolari del trattamento dovrebbero indicare, fra gli stabilimenti ove sono assunte decisioni in merito al trattamento, quello che disporrà della facoltà di ordinare l'esecuzione di tali decisioni con riguardo alla totalità dei contitolari del trattamento. Sarà quest'ultimo stabilimento a costituire lo stabilimento principale rispetto al trattamento svolto in contitolarità. L'accordo raggiunto fra i contitolari lascia impregiudicate le norme in materia di responsabilità previste nel regolamento, con particolare riguardo alle disposizioni dell'articolo 82, paragrafo 4.

2.2 CASI LIMITE

Possono esserci situazioni limite o particolarmente complesse in cui risulta difficile individuare lo stabilimento principale o stabilire dove sono prese le decisioni in merito ai trattamenti, per esempio quando c'è un trattamento transfrontaliero e il titolare del trattamento è stabilito in più Stati membri ma non ha un'amministrazione centrale nell'UE e nessuno degli stabilimenti nell'UE ha poteri decisionali rispetto al trattamento – ossia quando le decisioni sono prese al di fuori dell'UE.

In tal caso, la società che effettua trattamenti transfrontalieri ha probabilmente interesse a interagire con un'autorità capofila così da beneficiare del principio dello sportello unico. Tuttavia, il regolamento non offre una soluzione specifica; in situazioni del genere, la società dovrebbe designare come stabilimento principale quello che dispone della facoltà di ordinare l'esecuzione delle decisioni in materia di trattamento e assumersi le relative responsabilità, anche in termini di sufficienti risorse patrimoniali. Se la società non sceglie di designare uno stabilimento principale nei modi descritti, non sarà possibile individuare un'autorità capofila. Resta ferma la possibilità per le autorità di controllo di condurre ulteriori accertamenti se del caso.

Il regolamento non consente il "forum shopping": se una società afferma che il proprio stabilimento principale si trova un determinato Stato membro, ma tale stabilimento non svolge alcun esercizio reale ed effettivo di attività gestionali o decisionali rispetto al trattamento di dati personali, le autorità di controllo pertinenti (e, in ultima analisi, il Comitato) decideranno quale sia l'autorità di controllo "capofila" sulla base di criteri oggettivi e dell'analisi degli elementi probatori disponibili. Per determinare dove si trovi lo stabilimento principale potranno essere necessarie fattive attività di accertamento e collaborazio-

ne da parte delle autorità di controllo; la valutazione finale non può fondarsi esclusivamente sulle dichiarazioni rese dalla società o dal soggetto sotto esame. L'onere della prova ricade, in ultima analisi, su titolari del trattamento e responsabili del trattamento: questi dovrebbero essere in grado di dimostrare alle pertinenti autorità di controllo dove siano effettivamente assunte le decisioni che riguardano il trattamento di dati e dove si trovi la facoltà di ordinare l'esecuzione di tali decisioni. Un'efficace documentazione delle attività di trattamento faciliterebbe l'individuazione dell'autorità capofila tanto da parte delle società quanto da parte delle autorità di controllo. L'autorità di controllo capofila o le autorità interessate possono respingere l'analisi svolta dal titolare del trattamento, sulla base di un'analisi oggettiva dei fatti pertinenti, e chiedere, se necessario, informazioni ulteriori.

In alcuni casi le autorità di controllo pertinenti chiederanno al titolare del trattamento di fornire elementi inequivocabili – conformi alle linee guida eventualmente pubblicate dal Comitato europeo per la protezione dei dati – a dimostrazione del luogo dove si trova lo stabilimento principale ovvero dove sono prese le decisioni che riguardano un determinato trattamento. A questi elementi probatori sarà attribuito il giusto valore e le autorità di controllo individueranno congiuntamente quale di loro fungerà da capofila. Il Comitato sarà adito soltanto se, ai sensi dell'articolo 65, paragrafo 1, lettera b), le autorità non concorderanno sull'individuazione dell'autorità capofila; tuttavia, ci si attende che, nella maggioranza dei casi, le autorità siano in grado di definire un *modus operandi* con generale soddisfazione.

2.3 RESPONSABILI DEL TRATTAMENTO

Il regolamento consente di beneficiare del sistema di "sportello unico" anche ai responsabili del trattamento soggetti all'applicazione del regolamento stesso e con stabilimenti in più Stati membri.

In base all'articolo 4, punto 16, lettera b), del RGPD, lo stabilimento principale del responsabile del trattamento è il luogo della sua amministrazione centrale nell'UE ovvero, qualora non vi sia un'amministrazione centrale nell'UE, lo stabilimento nell'UE dove sono condotte le principali attività di trattamento di tale responsabile.

Tuttavia, in base al considerando 36, l'autorità di controllo capofila dovrebbe essere l'autorità capofila per il titolare del trattamento nei casi in cui in un trattamento siano coinvolti sia il titolare sia il responsabile del trattamento. In queste circostanze l'autorità di controllo competente per il responsabile del trattamento sarà un' "autorità interessata" e dovrebbe partecipare alla procedura di cooperazione. Questa regola troverà applicazione esclusivamente se il titolare del trattamento è stabilito nell'UE; se invece il titolare del trattamento è soggetto all'applicazione del regolamento sulla base di quanto dispone l'articolo 3, paragrafo 2, dello stesso, tale titolare sarà escluso dall'intervento del meccanismo di "sportello unico".

Un responsabile del trattamento può fornire servizi a più titolari situati in diversi Stati membri: si pensi, per esempio, a un importante fornitore di servizi cloud. In casi del genere, l'autorità di controllo capofila sarà quella competente a fungere da capofila nei riguardi del titolare del trattamento. Ciò significa, in ultima analisi, che un responsabile del trattamento potrà trovarsi a interagire con molteplici autorità di controllo.

3 ALTRE PROBLEMATICHE RILEVANTI

3.1 IL RUOLO DELL'"AUTORITÀ DI CONTROLLO INTERESSATA"

L'articolo 4, punto 22, del RGPD afferma quanto segue:

> *[si intende per] «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo.*

La nozione di "autorità di controllo interessata" è tesa a garantire che il principio dell'"autorità di controllo capofila" non impedisca ad altre autorità di controllo di esprimere il proprio punto di vista sull'approccio a una specifica problematica – per esempio, qualora persone residenti al di fuori del territorio di competenza dell'autorità di controllo capofila siano influenzate in modo sostanziale da un determinato trattamento. Per quanto riguarda la circostanza di cui alla lettera a), valgono le considerazioni già svolte rispetto all'individuazione dell'autorità di controllo capofila. Per quanto riguarda la condizione di cui alla lettera b), occorre rilevare che essa postula esclusivamente la residenza dell'interessato nello specifico Stato membro: non occorre, dunque, che si tratti di un cittadino di tale Stato membro. Nel caso di cui alla lettera c), non vi saranno generalmente difficoltà a stabilire se una determinata autorità di controllo abbia nei fatti ricevuto un reclamo.

In base all'articolo 56, paragrafi 2 e 5, del regolamento, l'autorità di controllo interessata ha voce in capitolo nella trattazione di un caso anche senza fungere da autorità di controllo capofila. Se l'autorità di controllo capofila decide di non trattare un caso, sarà l'autorità interessata che ne ha informato la capofila a occuparsene, nel rispetto delle procedure di cui all'articolo 61 (assistenza reciproca) e 62 (operazioni congiunte delle autorità di controllo) del regolamento. Una situazione del genere può configurarsi, ad esempio, nel caso in cui una società di marketing il cui stabilimento principale è situato a Parigi lanci un prodotto che produce i propri effetti soltanto su interessati che risiedono in Portogallo. In questo caso le autorità di controllo francese e portoghese potranno stabilire di comune accordo che è opportuno che sia l'autorità di controllo portoghese a gestire la questione. Le

autorità di controllo potranno chiedere ai titolari del trattamento di fornire chiarimenti rispetto agli accordi societari in essere. Poiché il trattamento produce effetti esclusivamente locali, ossia solo su interessati nel Portogallo, le due autorità di controllo sono libere di decidere se debba essere quella francese o quella portoghese a occuparsi del caso, conformemente al considerando 127.

Il RGPD impone all'autorità di controllo capofila e alle autorità di controllo interessate di collaborare tenendo in debita considerazione le rispettive posizioni, così da assicurare che le singole problematiche siano esaminate e risolte con mutua soddisfazione e garantendo una via di ricorso efficace agli interessati. Le autorità di controllo sono tenute a ricercare approcci che siano accettabili su base condivisa. Il meccanismo di coerenza dovrebbe entrare in gioco solo se il risultato delle attività di cooperazione non risulta accettabile per tutte le parti in causa.

La reciproca accettazione delle decisioni proposte vale tanto per le conclusioni sostanziali sul caso quanto per l'approccio che si sceglie di adottare – anche rispetto alle attività di indagine (che possono essere a tutto campo ovvero a raggio limitato). Lo stesso dicasi per l'eventuale decisione di non trattare un caso in conformità con il regolamento – per esempio in rapporto a priorità individuate ufficialmente da un'autorità, o a causa dell'esistenza di altre autorità interessate nei termini di cui sopra.

La ricerca di collegialità e un approccio collaborativo fra le autorità di controllo sono elementi essenziali ai fini della riuscita delle procedure di cooperazione e coerenza previste nel regolamento.

3.2 TRATTAMENTI LOCALI

I trattamenti di dati svolti in sede locale non ricadono nel campo di applicazione delle disposizioni del RGPD in materia di cooperazione e coerenza. Le autorità di controllo rispetteranno la competenza reciproca nella gestione su base locale dei trattamenti che hanno impatto locale. Anche i trattamenti svolti dalle autorità pubbliche saranno sempre gestiti su base "locale".

3.3 SOCIETÀ NON STABILITE NELL'UE

Il meccanismo di cooperazione e coerenza previsto dal RGPD si applica esclusivamente ai titolari del trattamento che abbiano uno o più stabilimenti nell'Unione europea. Se una società non dispone di uno stabilimento nell'UE, la semplice esistenza di un rappresentante designato in uno Stato membro non comporta l'intervento del meccanismo di "sportello unico". Ciò significa che un titolare del trattamento che non sia stabilito in alcun paese dell'UE dovrà interfacciarsi con le autorità di controllo di ciascuno Stato membro in cui opera, per il tramite del rappresentante designato.

Fatto a Bruxelles il 13 dicembre 2016

Per il Gruppo di lavoro,
La Presidente
Isabelle FALQUE-PIERROTIN

Versione emendata e adottata in data 5 aprile 2017

Per il Gruppo di lavoro
La Presidente
Isabelle FALQUE-PIERROTIN

ALLEGATO I
GUIDA ALL'INDIVIDUAZIONE DELL'AUTORITÀ DI CONTROLLO CAPOFILA

1. Il titolare del trattamento o il responsabile del trattamento effettua trattamenti transfrontalieri di dati personali?

a. Sì, se:

- il titolare del trattamento o il responsabile del trattamento è stabilito in più Stati membri dell'UE, e
- il trattamento di dati personali avviene nel contesto delle attività di stabilimenti situati in più Stati membri dell'UE.

➢ In tal caso, si vada al punto 2.

b. Sì, se:

- il trattamento di dati personali avviene nel contesto delle attività di un unico stabilimento del titolare del trattamento o del responsabile del trattamento nell'UE, ma tale trattamento:
- incide, o probabilmente incide, in modo sostanziale su interessati in più di uno Stato membro.

➢ In tal caso, l'autorità capofila è quella competente sull'unico stabilimento del titolare del trattamento o del responsabile del trattamento situato nello specifico Stato membro. Quest'ultimo, a termini di logica, è necessariamente lo stabilimento principale del titolare del trattamento o del responsabile del trattamento in quanto è l'unico stabilimento loro pertinente.

2. Individuazione dell'autorità di controllo capofila

a. Se è coinvolto solo un titolare del trattamento :

I. individuare il luogo della sua amministrazione centrale nell'UE;

II. l'autorità di controllo dello Stato membro dove si trova il luogo di amministrazione centrale del titolare del trattamento è l'autorità capofila per tale titolare.

Tuttavia:

III. se le decisioni su finalità e mezzi del trattamento sono prese in un altro stabilimento nell'UE, e tale stabilimento dispone della facoltà di ordinare l'esecuzione di tali decisioni, l'autorità capofila sarà quella situata nello Stato ove si trova tale altro stabilimento nell'UE.

b. Se sono coinvolti sia un titolare del trattamento sia un responsabile del trattamento :

I. verificare se il titolare del trattamento è stabilito nell'UE e soggetto al meccanismo di sportello unico. In caso affermativo,

II. individuare l'autorità di controllo capofila per il titolare del trattamento, che fungerà da autorità di controllo capofila anche per il responsabile del trattamento;

III. l'autorità di controllo (non capofila) competente per il responsabile del trattamento sarà un'autorità interessata – si veda il punto 3.

c. Se è coinvolto soltanto un responsabile del trattamento:

I. individuare il luogo della sua amministrazione centrale nell'UE;

II. qualora non vi sia un luogo di amministrazione centrale nell'UE, individuare lo stabilimento nell'UE nel contesto del quale si svolgono le principali attività di trattamento del responsabile.

d. Se sono coinvolti contitolari del trattamento:

I. verificare se i contitolari del trattamento sono stabiliti nell'UE;

II. designare, fra gli stabilimenti ove sono assunte decisioni in merito alle finalità e ai mezzi del trattamento, quello che dispone della facoltà di ordinare l'esecuzione di tali decisioni con riguardo alla totalità dei contitolari. Questo stabilimento sarà considerato lo stabilimento principale rispetto al trattamento svolto dai contitolari. L'autorità capofila è quella situata nel paese ove si colloca tale stabilimento.

3. Vi sono "autorità di controllo interessate"?

Un'autorità di controllo è un' "autorità di controllo interessata":

- qualora il titolare del trattamento o il responsabile del trattamento abbia uno stabilimento nel suo territorio, ovvero
- qualora il trattamento incida, o è probabile che incida, in modo sostanziale su interessati nel suo territorio, ovvero
- qualora riceva un reclamo.

NOTE

[1] Il regolamento rappresenta un atto rilevante ai fini del SEE e sarà applicabile una volta incorporato nell'Accordo SEE. La relativa analisi è in corso, si veda http://www.efta.int/eea-lex/32016R0679.

[2] Il Gruppo di lavoro è consapevole dell'esistenza di una molteplicità di trattamenti connessi all'attività bancaria. Tuttavia, in un'ottica di semplificazione, vengono raggruppati in questa sede sotto il profilo di una finalità unica. Lo stesso dicasi per i trattamenti svolti per finalità assicurative.

[3] Occorre ricordare, inoltre, che il regolamento prevede la possibilità di un controllo solo locale in casi specifici. Si veda il considerando 127: "***Ogni autorità di controllo che non agisce in qualità di autorità di controllo capofila dovrebbe essere competente a trattare casi locali*** *qualora il titolare del trattamento o il responsabile del trattamento sia stabilito in più di uno Stato membro, ma l'oggetto dello specifico trattamento riguardi* ***unicamente il trattamento effettuato in un singolo Stato membro e coinvolga soltanto interessati in tale singolo Stato membro****, ad esempio quando l'oggetto riguardi il trattamento di dati personali di dipendenti nell'ambito di specifici rapporti di lavoro in uno Stato membro."* Ciò significa che il controllo sul trattamento di dati relativi alle risorse umane nel contesto locale dei rapporti di lavoro potrebbe spettare a più autorità di controllo.

WP244 Allegato II - Domande frequenti

Chi è l'autorità di controllo capofila?

Il regolamento generale sulla protezione dei dati dispone che, di norma, il controllo dei trattamenti transfrontalieri o che coinvolgono cittadini di più paesi dell'UE è diretto da una sola autorità di controllo: l'autorità di controllo capofila. Si tratta del cosiddetto "principio dello sportello unico".
L'autorità di controllo capofila è l'organo cui spetta in prima battuta la gestione di un *trattamento transfrontaliero*, per esempio quando una società che effettua trattamenti in più Stati membri è oggetto di indagini.

L'autorità di controllo capofila coordina le operazioni che coinvolgono le autorità di controllo interessate, conformemente agli articoli da 60 a 62 del regolamento (ad esempio, sportello unico, assistenza reciproca, operazioni congiunte), e presenta un progetto di decisione alle autorità di controllo aventi un interesse nella questione.

Cos'è un trattamento transfrontaliero?

Il meccanismo dell'autorità di controllo capofila scatta soltanto nell'ambito di un trattamento transfrontaliero. Occorre pertanto stabilire se il trattamento in questione è un trattamento transfrontaliero.
Ai sensi dell'articolo 4, punto 23, del regolamento per "trattamento transfrontaliero" si intende:

- *[il] trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure*

- *[il] trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.*

Cosa significa "incide in modo sostanziale"?

Il regolamento non definisce cosa si debba intendere per "incide in modo sostanziale".

Nell'interpretare il senso dell'espressione "incide in modo sostanziale", le autorità di controllo devono valutare ciascun caso in rapporto alle specifiche circostanze, tenendo conto del contesto in cui si svolge il trattamento, del tipo di dati trattati, delle finalità del trattamento e di altri fattori, tra cui se il trattamento:

- è causa, o probabile causa, di una perdita, un danno o un disagio per la persona;
- produce concretamente, o è probabile che produca concretamente, una limitazione dei diritti o un'esclusione da benefici e opportunità;
- incide, o probabilmente incide, sulla salute, il benessere o la tranquillità della persona;
- incide, o probabilmente incide, sulla situazione economica o finanziaria della persona;
- espone la persona a forme di discriminazione o disparità di trattamento;
- comporta l'analisi di categorie particolari di dati personali o di altri dati che configurano un'ingerenza nella sfera privata, in particolare dati personali di minori;
- è causa, o probabile causa, di modifiche significative nella condotta della persona;
- genera conseguenze impreviste, inattese o indesiderate per la persona;
- provoca situazioni di imbarazzo o altre conseguenze negative, compreso il danno reputazionale;
- comporta il trattamento di un'ampia gamma di dati personali.

Come si individua l'autorità di controllo capofila in relazione al titolare del trattamento?

Una volta accertato che il trattamento in questione è un trattamento transfrontaliero, occorre individuare l'autorità di controllo capofila.

Ai sensi dell'articolo 56 del regolamento, l'autorità capofila è l'autorità di controllo del paese in cui si trova lo stabilimento principale dell'impresa.

Se un'impresa ha un unico stabilimento nell'UE, ma il trattamento incide o probabilmente incide in modo sostanziale sugli interessati in più di uno Stato membro, l'autorità di controllo capofila è l'autorità di controllo del luogo in cui si trova lo stabilimento unico.

Se un'impresa ha più stabilimenti nell'UE, di norma è considerato stabilimento principale il luogo dell'amministrazione centrale dell'impresa. Tuttavia, se le decisioni sulle finalità e i mezzi del trattamento sono prese in un altro stabilimento - che ha anche la facoltà di ordinare l'esecuzione di tali decisioni - quest'ultimo stabilimento diventa lo stabilimento principale. Spetta ai titolari del trattamento stabilire chiaramente dove sono prese le decisioni sulle finalità e i mezzi del trattamento dei dati personali.

A mo' di esempio, se un'impresa effettua uno o più trattamenti transfrontalieri e le decisioni su tutti i trattamenti transfrontalieri sono prese nel luogo dell'amministrazione centrale nell'UE, ci sarà un'unica autorità di controllo capofila per tutti i trattamenti transfrontalieri: l'autorità di controllo del luogo dell'amministrazione centrale dell'impresa.

Tuttavia, se un'impresa effettua più trattamenti transfrontalieri e le decisioni sulle finalità e i mezzi del trattamento sono prese in diversi stabilimenti, ci

saranno più autorità di controllo capofila: le autorità di controllo dei luoghi degli stabilimenti che prendono le decisioni sui rispettivi trattamenti transfrontalieri. Per beneficiare pienamente del meccanismo dello sportello unico, con un'unica autorità di controllo capofila per tutti i trattamenti transfrontalieri, le imprese dovrebbero prevedere di centralizzare i poteri decisionali sui trattamenti dei dati personali in un unico luogo.

Quali sono i criteri per individuare l'autorità di controllo capofila in relazione al titolare del trattamento?

Per determinare dove si trova lo stabilimento principale del responsabile del trattamento è utile ricorrere ai seguenti criteri:

- Il responsabile del trattamento ha un unico stabilimento nell'UE?

  Se sì, e se il trattamento incide o probabilmente incide in modo sostanziale sugli interessati in più di uno Stato membro, l'autorità di controllo capofila è l'autorità di controllo del luogo in cui si trova lo stabilimento unico.

- Il responsabile del trattamento ha uno stabilimento nell'UE?

  - Se sì, qual è il suo ruolo? le decisioni sulle finalità e i mezzi del trattamento sono prese in tale stabilimento e quest'ultimo ha la facoltà di ordinare l'esecuzione delle decisioni sul trattamento?

  - In caso negativo, ci sono altri stabilimenti in cui:

- sono prese le decisioni su attività societarie che comportano trattamenti di dati?
- si trova effettivamente la facoltà di ordinare l'esecuzione delle decisioni prese?
- si trova l'amministratore (o gli amministratori) cui spetta la responsabilità gestionale complessiva del trattamento transfrontaliero?
- risulta costituita la società titolare o responsabile del trattamento, se questa ha sede in un solo Stato?

Come si individua l'autorità di controllo capofila in relazione al responsabile del trattamento?

Il regolamento consente anche ai responsabili del trattamento cui esso si applica e che hanno stabilimenti in più di uno Stato membro di beneficiare del meccanismo dello sportello unico.

In base all'articolo 4, punto 16, lettera b), del regolamento lo stabilimento principale del responsabile del trattamento è il luogo della sua amministrazione centrale nell'UE ovvero, qualora non vi sia un'amministrazione centrale nell'UE, lo stabilimento nell'UE dove sono condotte le principali attività di trattamento di tale responsabile.

Tuttavia, in base al considerando 36, l'autorità di controllo capofila dovrebbe essere l'autorità capofila per il titolare del trattamento nei casi in cui in un trattamento siano coinvolti sia il titolare sia il responsabile del trattamento. In queste circostanze l'autorità di controllo competente per il responsabile del trattamento sarà considerata un'"autorità interessata" e dovrebbe partecipare alla procedura di cooperazione.

Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679 [WP 253]

Adottate il 3 ottobre 2017

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 di detta direttiva,

visto il proprio regolamento interno,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

Indice

I. INTRODUZIONE

L'UE ha attuato una riforma globale della normativa sulla protezione dei dati in Europa. La riforma si basa su diversi pilastri (componenti fondamentali): norme coerenti, procedure semplificate, azioni coordinate, coinvolgimento degli utenti, informazioni più efficaci e rafforzamento dei poteri destinati a far rispettare le norme.

I titolari del trattamento e i responsabili del trattamento[1] hanno maggiori responsabilità nel garantire l'efficace tutela dei dati personali delle persone fisiche. Le autorità di controllo sono dotate di poteri per garantire che i principi del regolamento generale sulla protezione dei dati (di seguito "il regolamento") e i diritti delle persone interessate siano rispettati conformemente all'enunciato e alla ratio del regolamento.

L'applicazione coerente delle norme sulla protezione dei dati è fondamentale per un regime di protezione dei dati armonizzato. Le sanzioni amministrative pecuniarie rappresentano un elemento centrale del nuovo regime introdotto dal regolamento per far rispettare le norme, in quanto costituiscono un componente importante dell'insieme di strumenti di applicazione a disposizione delle autorità di controllo, congiuntamente alle altre misure previste dall'articolo 58.

Il presente documento è destinato a essere utilizzato dalle autorità di controllo per garantire una migliore applicazione e attuazione del regolamento ed espone l'interpretazione comune delle disposizioni di cui all'articolo 83 del regolamento nonché l'interazione di detto articolo con gli articoli 58 e 70 e i relativi considerando.

In particolare, ai sensi dell'articolo 70, paragrafo 1, lettera e), il comitato europeo per la protezione dei dati ha la facoltà di pubblicare linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del regolamento, e l'articolo 70, paragrafo 1, lettera k), specifica che è prevista l'elaborazione di linee guida riguardanti la previsione di sanzioni amministrative pecuniarie.

Le presenti linee guida non sono esaustive e non forniscono spiegazioni in merito alle differenze esistenti tra sistemi amministrativi, civili o penali nell'imposizione di sanzioni amministrative in generale.

Al fine di adottare un approccio coerente all'imposizione di sanzioni amministrative pecuniarie, che rispecchi adeguatamente tutti i principi delle presenti linee guida, il comitato europeo per la protezione dei dati ha raggiunto un'intesa comune sui criteri di valutazione di cui all'articolo 83, paragrafo 2, del regolamento e, pertanto, il comitato e le singole autorità di controllo concordano sull'impiego delle presenti linee guida come approccio comune.

II. PRINCIPI

Una volta accertata la violazione del regolamento dopo aver valutato i fatti del caso, l'autorità di controllo competente deve individuare la o le misure correttive più appropriate per affrontare tale violazione. Le disposizioni di cui all'articolo 58, paragrafo 2, lettere da b) a j)[2], indicano gli strumenti che le autorità di controllo hanno a disposizione per far fronte a un'inadempienza da parte di un titolare del trattamento o responsabile del trattamento. Nel ricorrere a tali poteri, le autorità di controllo devono osservare i seguenti principi:

1. LA VIOLAZIONE DEL REGOLAMENTO DOVREBBE COMPORTARE L'IMPOSIZIONE DI "SANZIONI EQUIVALENTI".

Il concetto di "equivalenza" è fondamentale nel determinare la portata degli obblighi delle autorità di controllo di garantire coerenza nel ricorso ai poteri correttivi di cui all'articolo 58, paragrafo 2, in generale e nell'applicazione delle sanzioni amministrative in particolare[3].

Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, ***il livello di protezione dovrebbe essere equivalente*** *in tutti gli Stati membri* (considerando 10). Il considerando 11 spiega che per garantire un livello equivalente di protezione dei dati personali in tutta l'Unione occorrono, tra l'altro, *"poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri"*. Inoltre, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri sono considerate un modo per *"prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno"*, in linea con il considerando 13 del regolamento.

Il regolamento offre una base più solida rispetto alla direttiva 95/46/CE ai fini di una maggiore coerenza, in quanto esso è direttamente applicabile negli Stati membri. Anche se le autorità di controllo agiscono in "piena indipendenza" (articolo 52) nei confronti dei governi nazionali, dei titolari del trattamento o

dei responsabili del trattamento, esse devono collaborare *"al fine di garantire l'applicazione e l'attuazione coerente del presente regolamento"* (articolo 57, paragrafo 1, lettera g)).

Il regolamento esorta a una maggiore coerenza rispetto alla direttiva 95/46/CE nell'imposizione delle sanzioni. Nei casi transfrontalieri, la coerenza deve essere garantita principalmente mediante il meccanismo di cooperazione (sportello unico) e in una certa misura tramite il meccanismo di coerenza introdotto dal nuovo regolamento.

Nei casi nazionali previsti dal regolamento, le autorità di controllo applicheranno le presenti linee guida nello spirito di collaborazione ai sensi dell'articolo 57, paragrafo 1, lettera g), e dell'articolo 63, al fine di garantire la coerenza dell'applicazione e dell'attuazione del regolamento. Sebbene continuino a essere indipendenti nello scegliere le misure correttive di cui all'articolo 58, paragrafo 2, le autorità di controllo dovrebbero evitare di scegliere misure correttive differenti in casi analoghi.

Lo stesso principio si applica quando tali misure correttive sono imposte sotto forma di sanzioni pecuniarie.

2. COME TUTTE LE MISURE CORRETTIVE SCELTE DALLE AUTORITÀ DI CONTROLLO, LE SANZIONI AMMINISTRATIVE PECUNIARIE DOVREBBERO ESSERE "EFFETTIVE, PROPORZIONATE E DISSUASIVE".

Come tutte le misure correttive in generale, le sanzioni amministrative pecuniarie dovrebbero rispondere adeguatamente alla natura, alla gravità e alle conseguenze della violazione, e le autorità di controllo devono valutare tutte le circostanze del caso in maniera coerente e oggettivamente giustificata. La valutazione di quanto sia effettivo, proporzionato e dissuasivo in ciascun caso dovrà anche riflettere l'obiettivo perseguito dalla misura correttiva prescelta, che è quello di ripristinare la conformità alle norme oppure di punire un comportamento illecito (o entrambi).

Le autorità di controllo dovrebbero individuare misure correttive che siano *"effettive, proporzionate e dissuasive"* (articolo 83, paragrafo 1), sia nei casi nazionali (articolo 55) che nei casi che comportano il trattamento transfrontaliero dei dati (secondo la definizione di cui all'articolo 4, punto 23).

Le presenti linee guida riconoscono che la legislazione nazionale può stabilire requisiti aggiuntivi per la procedura che le autorità di controllo devono seguire per far rispettare le norme. Essi possono consistere ad esempio in notifiche di indirizzo, moduli, termini per presentare osservazioni, appello, esecuzione, pagamento[4].

Tali requisiti non dovrebbero tuttavia ostacolare in pratica il conseguimento degli obiettivi di efficacia, proporzionalità e dissuasività.

Una determinazione più precisa dell'efficacia, della proporzionalità e della dissuasività scaturirà dalla pratica che emergerà in seno alle autorità di controllo (in materia di protezione dei dati e grazie alle esperienze acquisite in altri settori normativi) e dalla giurisprudenza relativa all'interpretazione di tali principi.

Al fine di irrogare sanzioni amministrative che siano effettive, proporzionate e dissuasive, l'autorità di controllo deve rifarsi alla definizione della nozione di impresa fornita dalla Corte di giustizia dell'Unione europea (CGUE) ai fini dell'applicazione degli articoli 101 e 102 TFUE, secondo cui il concetto di impresa va inteso come un'unità economica che può essere composta dall'impresa madre e da tutte le filiali coinvolte. Conformemente al diritto e alla giurisprudenza dell'UE[5], un'impresa deve essere intesa quale unità economica che intraprende attività economiche/commerciali, a prescindere dalla persona giuridica implicata (considerando 150).

3. L'AUTORITÀ DI CONTROLLO COMPETENTE EFFETTUERÀ UNA VALUTAZIONE "IN OGNI SINGOLO CASO".

È possibile imporre sanzioni amministrative pecuniarie in risposta a una vasta serie di violazioni. L'articolo 83 del regolamento prevede un approccio armonizzato nei confronti delle violazioni di obblighi espressamente elencate nei paragrafi da 4 a 6. Il diritto di uno Stato membro può estendere l'applicazione dell'articolo 83 alle autorità e agli organismi pubblici istituiti in tale Stato membro. Inoltre, il diritto di uno Stato membro può consentire o addirittura imporre l'irrogazione di una sanzione pecuniaria in caso di violazione di disposizioni diverse da quelle citate all'articolo 83, paragrafi da 4 a 6.

Il regolamento stabilisce che ogni caso sia valutato singolarmente[6]. L'articolo 83, paragrafo 2, rappresenta il punto di partenza di tale valutazione individuale. Esso prevede che *"al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi..."*. Di conseguenza, e alla luce del considerando 148[7], l'autorità di controllo ha la responsabilità di scegliere la o le misure più appropriate. Nei casi citati all'articolo 83, paragrafi da 4 a 6, tale scelta deve tenere conto di tutte le misure correttive, tra cui l'imposizione della sanzione amministrativa pecuniaria appropriata, sia che essa sia associata a una misura correttiva ai sensi dell'articolo 58, paragrafo 2, oppure che sia autonoma.

Le sanzioni pecuniarie rappresentano un importante strumento che le autorità di controllo dovrebbero utilizzare nelle opportune circostanze. Le autorità di controllo sono incoraggiate a ricorrere alle misure correttive con un approccio ponderato ed equilibrato, al fine di reagire in maniera effettiva, dissuasiva e proporzionata alla violazione. Il punto non è qualificare le sanzioni pecuniarie come misure di ultima istanza, né evitare di irrogarle, bensì utilizzarle in un modo che non ne riduca l'efficacia come strumento.

Il comitato europeo per la protezione dei dati, negli ambiti di sua competenza ai sensi dell'articolo 65 del regolamento, adotterà una decisione vincolante sulle controversie tra le autorità, in particolare in merito alla determinazione dell'esistenza di una violazione. Se un'obiezione pertinente e motivata mette in discussione la conformità di una misura correttiva con il regolamento generale sulla protezione dei dati, la decisione del comitato europeo per la protezione dei dati esaminerà anche in che modo la sanzione amministrativa pecuniaria proposta nel progetto di decisione dell'autorità di controllo competente rispetta i principi di efficacia, proporzionalità e deterrenza. Seguiranno separatamente orientamenti del comitato europeo per la protezione dei dati sull'applicazione dell'articolo 65 del regolamento per ulteriori dettagli sul tipo di decisione che il comitato deve adottare.

4. UN APPROCCIO ARMONIZZATO ALLE SANZIONI AMMINISTRATIVE PECUNIARIE IN MATERIA DI PROTEZIONE DEI DATI RICHIEDE LA PARTECIPAZIONE ATTIVA DELLE AUTORITÀ DI CONTROLLO E LO SCAMBIO DI INFORMAZIONI TRA LE STESSE.

Le presenti linee guida riconoscono che per alcune autorità di controllo nazionali i poteri sanzionatori rappresentano una novità nel settore della protezione dei dati e sollevano numerose questioni in termini di risorse, organizzazione e procedura. In particolare, le decisioni in cui le autorità di controllo esercitano i poteri sanzionatori saranno impugnabili dinanzi ai tribunali nazionali.

Le autorità di controllo collaborano tra loro e, ove necessario, con la Commissione europea tramite il meccanismo di cooperazione, come stabilito nel regolamento, al fine di sostenere scambi formali e informali di informazioni, ad esempio attraverso seminari periodici. Tale cooperazione si concentrerà sulla loro esperienza e pratica nell'applicazione dei poteri sanzionatori al fine di raggiungere una maggiore coerenza.

Questa condivisione attiva di informazioni, insieme alla giurisprudenza emergente sul ricorso a tali poteri, potrebbe condurre a una rivisitazione dei principi o dei dettagli particolari delle presenti linee guida.

III. CRITERI DI VALUTAZIONE DI CUI ALL'ARTICOLO 83, PARAGRAFO 2

L'articolo 83, paragrafo 2, contiene un elenco di criteri che le autorità di controllo devono usare per valutare sia l'opportunità di irrogare una sanzione amministrativa che l'importo della sanzione. Ciò non significa che occorre ripetere la valutazione usando gli stessi criteri, bensì che si deve procedere a una valutazione che tenga conto di tutte le circostanze di ogni singolo caso, conformemente all'articolo 83[8].

Le conclusioni raggiunte nella prima fase della valutazione possono essere impiegate nella seconda parte relativa all'importo della sanzione, evitando così di dover eseguire la valutazione utilizzando gli stessi criteri due volte.

La presente sezione fornisce orientamenti alle autorità di controllo su come interpretare le singole circostanze del caso alla luce dei criteri di cui all'articolo 83, paragrafo 2.

a) la natura, la gravità e la durata della violazione

Quasi tutti gli obblighi dei titolari del trattamento e dei responsabili del trattamento previsti dal regolamento sono classificati in base alla loro **natura** nelle disposizioni di cui all'articolo 83, paragrafi da 4 a 6. Il regolamento, fissando due diversi massimali per le sanzioni amministrative pecuniarie (10/20 milioni di EUR), fornisce già un'indicazione del fatto che la violazione di alcune disposizioni del regolamento può essere più grave della violazione di altre disposizioni. Tuttavia l'autorità di controllo competente, valutando le circostanze del caso alla luce dei criteri generali di cui all'articolo 83, paragrafo 2, può decidere che in quel particolare caso vi sia una necessità maggiore o minore di reagire con una misura correttiva sotto forma di sanzione pecuniaria. Quando è scelta una sanzione pecuniaria quale misura correttiva appropriata, da sola o in aggiunta ad altre misure, si applicherà il sistema a livelli del regolamento (articolo 83, paragrafi da 4 a 6) per individuare la sanzione massima imponibile a seconda della natura della violazione in questione.

Il considerando 148 introduce la nozione di "violazioni minori". Tali violazioni possono consistere nella violazione di una o più disposizioni del regolamento elencate all'articolo 83, paragrafo 4 o 5. La valutazione dei criteri di cui all'articolo 83, paragrafo 2, può tuttavia spingere l'autorità di controllo a ritenere che nelle circostanze concrete del caso la violazione, ad esempio, non crei un rischio significativo per i diritti degli interessati in questione e non incida sull'essenza dell'obbligo in questione. In tali casi, la sanzione può essere sostituita (ma non sempre) da un ammonimento.

Il considerando 148 non prevede l'obbligo per l'autorità di controllo di sostituire sempre una sanzione con un ammonimento in caso di violazione minore (*"potrebbe essere rivolto un ammonimento anziché imposta una sanzione pecuniaria"*), ma piuttosto una possibilità, dopo la valutazione concreta di tutte le circostanze del caso.

Il considerando 148 offre la stessa possibilità di sostituire una sanzione pecuniaria con un ammonimento qualora il titolare del trattamento sia una persona fisica e la sanzione pecuniaria che dovrebbe essere imposta costituisca un onere sproporzionato. L'autorità di controllo deve innanzitutto decidere, valutando le circostanze del caso, in merito alla necessità di irrogare una sanzione. Qualora sia favorevole a imporre una sanzione pecuniaria, l'autorità di controllo deve altresì valutare se la sanzione che dovrebbe essere imposta costituisca un onere sproporzionato per una persona fisica.

Il regolamento non fissa un importo specifico per violazioni specifiche, ma solo un massimale. Da ciò si può desumere la gravità relativamente minore delle violazioni di cui all'articolo 83, paragrafo 4, rispetto a quelle di cui all'ar-

ticolo 83, paragrafo 5. La reazione effettiva, proporzionata e dissuasiva a una violazione dell'articolo 83, paragrafo 5, dipenderà tuttavia dalle circostanze del caso.

Occorre notare che, in determinate circostanze, le violazioni del regolamento che per natura dovrebbero rientrare nella categoria *"fino a 10 000 000 EUR o [...] fino al 2 % del fatturato mondiale totale annuo"* conformemente all'articolo 83, paragrafo 4, potrebbero essere classificate in una categoria superiore (20 milioni di EUR). È il caso, ad esempio, di una violazione che sia stata precedentemente oggetto di un ordine[9] dell'autorità di controllo che il titolare o il responsabile del trattamento non ha rispettato[10] (articolo 83, paragrafo 6). Le disposizioni del diritto nazionale possono nella pratica ripercuotersi sulla valutazione[11]. La natura della violazione e *"l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito"* forniranno un'indicazione della gravità della violazione. Qualora nell'ambito di un singolo caso siano state commesse congiuntamente più violazioni diverse, l'autorità di controllo può applicare le sanzioni amministrative pecuniarie a un livello che risulti effettivo, proporzionato e dissuasivo entro i limiti della violazione più grave. Ad esempio, qualora siano stati violati l'articolo 8 e l'articolo 12, l'autorità di controllo può applicare le misure correttive di cui all'articolo 83, paragrafo 5, che corrispondono alla categoria della violazione più grave, ossia quella dell'articolo 12. Precisare ulteriori dettagli in questa fase esula dall'ambito delle presenti linee guida (un calcolo più dettagliato costituirebbe l'oggetto di un'eventuale fase successiva delle presenti linee guida).

I fattori presentati di seguito devono essere valutati combinatamente, ad esempio il numero di interessati va valutato in combinazione con le possibili ripercussioni nei loro confronti.

Occorre valutare il **numero** di interessati coinvolti, al fine di stabilire se si tratta di un evento isolato oppure del sintomo di una violazione sistemica oppure dell'assenza di prassi adeguate. Ciò non vuol dire che gli eventi isolati non debbano essere punibili, in quanto un evento isolato potrebbe pur sempre ripercuotersi su molti interessati. A seconda delle circostanze del caso, ciò dipenderà, ad esempio, dal numero totale di soggetti registrati nella banca dati in questione, dal numero di utenti di un servizio, dal numero di clienti, oppure dalla popolazione del paese, ove opportuno.

Occorre altresì valutare la finalità del trattamento. Il parere del Gruppo di lavoro sulla "limitazione delle finalità"[12] ha analizzato i due elementi fondamentali di tale principio della normativa sulla protezione dei dati: indicazione specifica della finalità e utilizzo compatibile. Nel valutare la finalità del trattamento nel contesto dell'articolo 83, paragrafo 2, le autorità di controllo dovrebbero valutare la misura in cui il trattamento rispetta i due elementi fondamentali del suddetto principio[13]. In alcuni casi, l'autorità di controllo potrebbe ritenere necessario inserire un'analisi più approfondita della finalità del trattamento stesso nell'analisi dell'articolo 83, paragrafo 2.

Se gli interessati hanno subito un **danno**, occorre considerarne l'entità. Il trattamento dei dati personali può generare rischi per i diritti e le libertà personali, come esposto al considerando 75:

> *"I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati."*

Se dalla violazione del regolamento sono sorti o potrebbero sorgere danni, l'autorità di controllo dovrebbe tenerne conto nella scelta della misura correttiva, sebbene non abbia la facoltà di corrispondere il risarcimento specifico del danno.

L'irrogazione di una sanzione pecuniaria non dipende dalla capacità dell'autorità di controllo di stabilire un nesso causale tra la violazione e il danno materiale (si veda ad esempio l'articolo 83, paragrafo 6).

La durata dell'infrazione può fornire un'indicazione, ad esempio, dei seguenti elementi:

a) condotta intenzionale da parte del titolare del trattamento, oppure

b) mancata adozione di misure preventive appropriate, oppure

c) incapacità di attuare le misure tecniche e organizzative richieste.

b) il carattere doloso o colposo della violazione

In generale, il "dolo" comprende sia la consapevolezza che l'intenzionalità in relazione alle caratteristiche di un reato, mentre per "colposo" si intende che non vi era l'intenzione di causare la violazione nonostante il titolare/responsabile del trattamento abbia violato l'obbligo di diligenza previsto per legge.

È generalmente riconosciuto che le violazioni dolose, da cui emerge il disprezzo per le disposizioni di legge, sono più gravi di quelle colpose e pertanto possono verosimilmente giustificare l'applicazione di una sanzione amministrativa pecuniaria. Le conclusioni circa il dolo o la colpa dipenderanno dagli elementi oggettivi di condotta rilevati dalle circostanze del caso. Inoltre, la giurisprudenza emergente e la pratica in materia di protezione dei dati nell'ambito dell'applicazione del regolamento chiariranno le circostanze fornendo linee di demarcazione più chiare per valutare il carattere doloso di una violazione.

Tra le circostanze indicanti il carattere doloso di una violazione figura il trattamento illecito autorizzato esplicitamente dall'alta dirigenza del titolare del trattamento oppure effettuato nonostante i pareri del responsabile della protezione dei dati o ignorando le politiche esistenti, ad esempio ottenendo e trattando dati relativi ai dipendenti di un concorrente con l'intento di screditare tale concorrente sul mercato.

Altri esempi sono:

- modifica di dati personali per dare un'impressione fuorviante (positiva) circa il conseguimento degli obiettivi – episodio riscontrato nel contesto degli obiettivi relativi ai tempi d'attesa ospedalieri;
- scambio di dati personali con finalità di marketing, ossia vendita di dati come "approvati" senza verificare/ignorando il parere degli interessati circa le modalità di utilizzo dei propri dati.

Altre circostanze, quali mancata lettura e non rispetto delle politiche esistenti, errore umano, mancata verifica dei dati personali nelle informazioni pubblicate, incapacità di apportare aggiornamenti tecnici in maniera puntuale, mancata adozione delle politiche (piuttosto che la semplice mancata applicazione) possono essere sintomo di negligenza.

Le imprese dovrebbero essere responsabili dell'adozione di strutture e risorse idonee alla natura e alla complessità della propria attività. Pertanto, i titolari del trattamento e i responsabili del trattamento non possono legittimare violazioni della normativa sulla protezione dei dati appellandosi a una carenza di risorse. Le prassi e la documentazione delle attività di trattamento seguono un approccio basato sul rischio ai sensi del regolamento.

Esistono zone grigie che influenzano il processo decisionale circa la necessità di imporre o meno una misura correttiva e l'autorità potrebbe dover condurre indagini più approfondite per accertare le circostanze del caso e per garantire che tutte le circostanze specifiche di ciascun caso siano state adeguatamente considerate.

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

I titolari del trattamento e i responsabili del trattamento hanno l'obbligo di attuare misure tecniche e organizzative volte a garantire un livello di sicurezza

adeguato al rischio, di condurre valutazioni di impatto sulla protezione dei dati e di mitigare i rischi arrecati ai diritti e alle libertà personali dal trattamento dei dati personali. Tuttavia, quando si verifica una violazione e l'interessato ne subisce i danni, la parte responsabile dovrebbe fare quanto in suo potere per ridurre le conseguenze della violazione per il o i soggetti coinvolti. Tale comportamento responsabile (o la sua assenza) sarà preso in considerazione dall'autorità di controllo nella scelta della o delle misure correttive e nel calcolo della sanzione da imporre nel caso specifico.

Sebbene i fattori attenuanti o aggravanti siano particolarmente utili per adeguare l'importo della sanzione amministrativa pecuniaria alle particolari circostanze del caso, il loro ruolo nella scelta della misura correttiva appropriata non dovrebbe essere sottovalutato. Nei casi in cui la valutazione fondata su altri criteri lascia l'autorità di controllo nel dubbio circa l'appropriatezza di una sanzione amministrativa pecuniaria, come misura correttiva a sé stante oppure in combinazione con altre misure di cui all'articolo 58, le circostanze aggravanti o attenuanti possono aiutare a scegliere le misure appropriate spostando l'ago della bilancia in favore di quella che sembra essere la misura più effettiva, proporzionata e dissuasiva nel caso in questione.

Tale disposizione serve per valutare il grado di responsabilità del titolare del trattamento in seguito al verificarsi di una violazione. Può riguardare casi in cui è indubbio che il titolare/responsabile del trattamento non ha adottato un approccio imprudente/negligente e ha fatto quanto in suo potere per correggere le proprie azioni quando si è reso conto della violazione.

In passato, l'esperienza disciplinare delle autorità di controllo nell'ambito della direttiva 95/46/CE ha dimostrato che può essere opportuno mostrare un certo livello di flessibilità nei confronti di quei titolari/responsabili del trattamento che hanno ammesso la violazione e che si sono assunti la responsabilità di correggere o limitare l'impatto delle loro azioni. Alcuni esempi potrebbero essere i seguenti (anche se non porterebbero in tutti i casi a un approccio più flessibile):

- aver contattato altri titolari/responsabili del trattamento che potrebbero essere stati coinvolti in un'estensione del trattamento, ad esempio nel caso in cui alcuni dati sono stati erroneamente condivisi con terze parti;

- azione tempestiva adottata dal titolare/responsabile del trattamento per impedire la prosecuzione o l'espansione della violazione a un livello o a una fase che avrebbe determinato ripercussioni ben più gravi.

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

Il regolamento ha introdotto un livello ben superiore di responsabilità del titolare del trattamento rispetto alla direttiva 95/46/CE sulla protezione dei dati.

Il grado di responsabilità del titolare del trattamento o del responsabile del trattamento valutato sulla base dell'adozione di una misura correttiva appropriata può dipendere dai seguenti aspetti:

- Il titolare del trattamento ha attuato misure tecniche che seguono i principi della protezione dei dati fin dalla progettazione o per impostazione predefinita (articolo 25)?
- Il titolare del trattamento ha attuato misure organizzative che attuano i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita (articolo 25) a tutti i livelli dell'organizzazione?
- Il titolare/responsabile del trattamento ha messo in atto un livello di sicurezza adeguato (articolo 32)?
- Le prassi/politiche pertinenti in materia di protezione dei dati sono conosciute e applicate al livello adeguato di gestione dell'organizzazione? (articolo 24).

L'articolo 25 e l'articolo 32 del regolamento prevedono che i titolari del trattamento tengano conto *"della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche"*. Anziché imporre un obbligo di risultato, tali disposizioni introducono obblighi di mezzi, il che significa che il titolare del trattamento deve condurre le valutazioni necessarie e giungere alle opportune conclusioni. La domanda cui l'autorità di controllo deve quindi rispondere è la seguente: in che misura il titolare del trattamento ha fatto quanto ci si aspettava facesse, considerando la natura, le finalità o l'entità del trattamento, alla luce degli obblighi imposti dal regolamento?

In tale valutazione, occorre tenere in debita considerazione qualsiasi procedura e metodo basati sulle migliori prassi, ove esistano e siano applicate. È importante tenere conto delle norme industriali e dei codici di condotta nel rispettivo campo o professione. I codici di condotta potrebbero fornire un'indicazione delle pratiche comuni nel settore e un'indicazione del livello di conoscenza dei diversi mezzi esistenti per affrontare le tipiche problematiche di sicurezza associate al trattamento.

Anche se le migliori prassi dovrebbero rappresentare l'ideale da perseguire in generale, nel valutare il grado di responsabilità occorre considerare le circostanze specifiche del singolo caso.

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

Tale criterio serve per valutare i precedenti dell'entità che commette la violazione. Le autorità di controllo dovrebbero considerare che la valutazione può

avere una portata piuttosto vasta poiché ogni tipo di violazione del regolamento, seppur di natura diversa da quella esaminata dall'autorità di controllo, potrebbe essere pertinente ai fini della valutazione, in quanto potrebbe fornire indicazioni su un livello generale di conoscenza insufficiente o di indifferenza nei confronti delle norme sulla protezione dei dati.

L'autorità di controllo dovrebbe valutare quanto segue:

- Il titolare/responsabile del trattamento ha già commesso la stessa violazione in precedenza?
- Il titolare/responsabile del trattamento ha commesso una violazione del regolamento secondo le stesse modalità? (ad esempio a causa di una conoscenza insufficiente delle prassi esistenti nell'organizzazione, oppure in seguito a una valutazione del rischio inadeguata, non rispondendo alle richieste dell'interessato in maniera tempestiva o per un ritardo ingiustificato nel rispondere alle richieste, ecc.).

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

L'articolo 83, paragrafo 2, prevede che il grado di cooperazione debba essere tenuto in "debito conto" al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa. Il regolamento non indica con precisione come tenere conto degli sforzi dei titolari del trattamento o dei responsabili del trattamento nel rimediare a una violazione già accertata dall'autorità di controllo. Inoltre, è chiaro che i criteri saranno solitamente applicati nel calcolo dell'importo della sanzione pecuniaria da imporre.

Tuttavia, nello scegliere la misura correttiva proporzionata al singolo caso si dovrebbe tener conto anche dell'eventuale l'intervento con cui il titolare del trattamento abbia limitato o addirittura azzerato le ripercussioni negative sui diritti delle persone che si sarebbero altrimenti verificate.

Un caso in cui la collaborazione con l'autorità di controllo potrebbe essere presa in debita considerazione è il seguente:

- L'entità ha risposto in modo particolare alle richieste dell'autorità di controllo durante la fase di indagine nel caso specifico limitando in tal modo in maniera significativa le ripercussioni sulle persone?

Detto ciò, non sarebbe opportuno tenere ulteriormente conto della collaborazione già prevista per legge: ad esempio, l'entità è in ogni caso tenuta a consentire all'autorità di controllo di accedere ai locali per controlli/ispezioni.

g) le categorie di dati personali interessate dalla violazione;

Alcuni esempi di domande chiave a cui l'autorità di controllo potrebbe ritenere necessario rispondere, ove opportuno, sono i seguenti:

- La violazione riguarda il trattamento di categorie particolari di dati di cui agli articoli 9 e 10 del regolamento?
- I dati sono direttamente/indirettamente identificabili?
- Il trattamento riguarda dati la cui diffusione causerebbe immediati danni/disagi alla persona (che non rientrano nelle categorie di cui agli articoli 9 e 10)?
- I dati sono direttamente disponibili senza protezioni tecniche oppure sono criptati[14]?

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

L'autorità di controllo potrebbe venire a conoscenza della violazione in seguito a indagini, reclami, articoli di giornale, suggerimenti anonimi oppure notifiche da parte del titolare del trattamento. Il titolare del trattamento ha l'obbligo a norma del regolamento di notificare all'autorità di controllo eventuali violazioni dei dati personali. Qualora il titolare del trattamento si limiti ad adempiere a tale obbligo, la conformità ad esso non può essere interpretata come fattore attenuante/mitigante. Analogamente, qualora il titolare/responsabile del trattamento abbia agito incautamente senza notificare la violazione, o perlomeno senza notificarne tutti i dettagli, in quanto non in grado di valutarne adeguatamente la portata, l'autorità di controllo potrebbe ritenere necessaria l'imposizione di una sanzione più grave, il che significa che risulterà improbabile la classificazione quale violazione minore.

i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

Il titolare del trattamento o il responsabile del trattamento potrebbe già essere nel mirino dell'autorità di controllo per la verifica della conformità in seguito a una precedente violazione. In tal caso gli eventuali precedenti contatti con il responsabile della protezione dei dati saranno stati verosimilmente numerosi e l'autorità di controllo li terrà in considerazione.

A differenza dei criteri di cui alla lettera e), questo criterio di valutazione serve solo per ricordare alle autorità di controllo di fare riferimento alle misure precedentemente emesse nei confronti del medesimo titolare o responsabile del trattamento "relativamente allo stesso oggetto".

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42;

Le autorità di controllo hanno il dovere di *"sorveglia[re] e assicura[re] l'applicazione del [...] regolamento"* (articolo 57, paragrafo 1, lettera a)). L'adesione ai codici di condotta approvati può essere utilizzata dal titolare del trattamen-

to o dal responsabile del trattamento per dimostrare la conformità, ai sensi dell'articolo 24, paragrafo 3, dell'articolo 28, paragrafo 5, o dell'articolo 32, paragrafo 3.
In caso di violazione di una delle disposizioni del regolamento, l'adesione a un codice di condotta approvato può fornire indicazioni circa la portata della necessità di intervenire con una sanzione amministrativa pecuniaria effettiva, proporzionata, dissuasiva o altra misura correttiva da parte dell'autorità di controllo. I codici di condotta approvati conterranno, ai sensi dell'articolo 40, paragrafo 4, *"i meccanismi che consentono all'organismo (di controllo) di effettuare il controllo obbligatorio del rispetto delle norme del codice"*.

Qualora il titolare del trattamento o il responsabile del trattamento abbia aderito a un codice di condotta approvato, l'autorità di controllo potrebbe ritenere sufficiente che la comunità incaricata di gestire il codice intervenga adeguatamente in prima persona nei confronti del proprio membro, ad esempio tramite i regimi di monitoraggio e applicazione del codice di condotta stesso. Pertanto, l'autorità di controllo potrebbe ritenere che tali misure siano sufficientemente effettive, proporzionate e dissuasive in quel particolare caso senza che l'autorità di controllo stessa debba imporre misure aggiuntive. Alcune forme di sanzionamento dei comportamenti non conformi possono avvenire tramite il regime di monitoraggio, ai sensi dell'articolo 41, paragrafo 2, lettera c), e dell'articolo 42, paragrafo 4), compresa la sospensione o l'esclusione del titolare del trattamento o del responsabile del trattamento dalla comunità incaricata di gestire il codice. Ciononostante, i poteri dell'organismo di controllo si espletano *"fatti salvi i compiti e i poteri dell'autorità di controllo competente"*, il che significa che l'autorità di controllo non ha l'obbligo di tenere conto delle sanzioni precedentemente imposte relative al regime di autoregolamentazione.

La non conformità con le misure di autoregolamentazione potrebbe altresì rivelare la colpa o il dolo del titolare/responsabile del trattamento.

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

La disposizione stessa fornisce esempi di quali altri elementi potrebbero essere presi in considerazione nel decidere l'appropriatezza di una sanzione amministrativa pecuniaria per una violazione delle disposizioni di cui all'articolo 83, paragrafi da 4 a 6.

Le informazioni relative ai profitti derivanti da una violazione potrebbero risultare particolarmente importanti per le autorità di controllo in quanto il guadagno economico derivante dalla violazione non può essere compensato tramite misure che non abbiano una componente pecuniaria. Pertanto, il fatto che il titolare del trattamento abbia tratto profitto dalla violazione del regolamento può costituire una chiara indicazione della necessità di imporre una sanzione pecuniaria.

IV. CONCLUSIONI

Le riflessioni sugli aspetti esposti nella sezione precedente aiuteranno le autorità di controllo a individuare, tra i fatti pertinenti del caso, i criteri più utili per valutare se sia necessario imporre una sanzione amministrativa pecuniaria appropriata in aggiunta o in sostituzione delle misure di cui all'articolo 58. Tenendo conto del contesto fornito dalla valutazione, l'autorità di controllo individuerà la misura correttiva più effettiva, proporzionata e dissuasiva per far fronte alla violazione.

L'articolo 58 fornisce alcuni orientamenti sulle misure tra cui un'autorità di controllo può scegliere, in quanto le misure correttive di per sé hanno natura diversa e sono destinate principalmente a finalità diverse. Alcune misure di cui all'articolo 58 possono anche essere cumulate, dando così luogo a un intervento che prevede più di una misura correttiva.

Non è sempre necessario integrare la misura con un'altra misura correttiva. Ad esempio, tenuto debito conto di cosa è proporzionato al caso specifico, l'efficacia e la dissuasività dell'intervento dell'autorità di controllo potrebbero essere garantite attraverso la sola sanzione pecuniaria.

In sintesi, le autorità devono ripristinare la conformità tramite tutte le misure correttive che hanno a disposizione. Le autorità di controllo dovranno altresì scegliere il canale più appropriato per portare avanti l'intervento (potendo ricorrere, ad esempio, a sanzioni penali - ove disponibili a livello nazionale).

La pratica di applicare sanzioni amministrative pecuniarie coerentemente all'interno dell'Unione europea è una pratica in via di evoluzione. Le autorità di controllo dovrebbero collaborare costantemente per aumentare tale coerenza, ad esempio tramite regolari scambi durante seminari sul trattamento dei casi o altri eventi che consentano di confrontare i casi a livello sub-nazionale, nazionale e transfrontaliero. Al fine di sostenere questa attività continuativa si raccomanda la creazione di un sottogruppo permanente annesso a una parte pertinente del comitato europeo per la protezione dei dati.

NOTE

[1] NdT: La versione italiana del regolamento (UE) 2016/679 ha modificato alcuni termini della direttiva 95/46/CE (abrogata dal regolamento stesso). Per coerenza terminologica, questo testo riprende sempre la terminologia del regolamento. Pertanto "controller" è il "titolare del trattamento" ("responsabile del trattamento" nella direttiva) e "processor" è il "responsabile del trattamento" ("incaricato del trattamento" nella direttiva).

[2] L'articolo 58, paragrafo 2, stabilisce che è possibile rivolgere avvertimenti quando "i trattamenti previsti possono verosimilmente violare le disposizioni del regolamento". In altre parole, nel caso contemplato dalla disposizione, la violazione del regolamento non è ancora avvenuta.

[3] Anche quando i sistemi giuridici di alcuni paesi dell'UE non consentono l'irrogazione di sanzioni amministrative pecuniarie come previsto dal regolamento, l'applicazione di tali norme in detti Stati membri deve avere effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo (considerando 151). Le autorità giurisdizionali sono vincolate dal regolamento ma non sono vincolate dalle presenti linee guida del comitato europeo per la protezione dei dati.

[4] Ad esempio, il quadro costituzionale e la proposta legislativa in materia di protezione dei dati dell'Irlanda prevedono che, prima di valutare la portata della o delle sanzioni, si giunga a una decisione formale in merito alla violazione stessa e la si comunichi alle parti interessate. La decisione sulla violazione non può essere rivista durante la valutazione della portata della o delle sanzioni.

[5] La definizione della giurisprudenza della Corte di giustizia è la seguente: "la nozione di impresa abbraccia qualsiasi entità che esercita un'attività economica, a prescindere dallo status giuridico di detta entità e dalle sue modalità di finanziamento" (causa Höfner e Elsner, punto 21, ECLI:EU:C:1991:161). Un'impresa "dev'essere intesa nel senso che essa si riferisce ad un'unità economica, anche qualora, sotto il profilo giuridico, questa unità economica sia costituita da più persone, fisiche o giuridiche" (causa Confederación Española de Empresarios de Estaciones de Servicio, punto 40, ECLI:EU-:C:2006:784).

[6] Oltre all'applicazione dei criteri di cui all'articolo 83, esistono altre disposizioni a sostegno di tale approccio quali:
considerando 141: *"Successivamente al reclamo si dovrebbe condurre un'indagine, soggetta a controllo giurisdizionale, nella misura in cui ciò sia opportuno nel caso specifico"*;
considerando 129: *"È opportuno che i poteri delle autorità di controllo siano esercitati nel rispetto di garanzie procedurali adeguate previste dal diritto dell'Unione e degli Stati membri, in modo imparziale ed equo ed entro un termine ragionevole. In particolare ogni misura dovrebbe essere appropriata, necessaria e proporzionata al fine di assicurare la conformità al presente regolamento, tenuto conto delle circostanze di ciascun singolo caso…"*;
articolo 57, paragrafo 1, lettera f): *"tratta i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'articolo 8, e svolge le indagini opportune sull'oggetto del reclamo"*.

[7] *"Per rafforzare il rispetto delle norme del presente regolamento, dovrebbero essere imposte sanzioni, comprese sanzioni amministrative pecuniarie per violazione del regolamento, in aggiunta o in sostituzione di misure appropriate imposte dall'autorità di controllo ai sen-*

si del presente regolamento. In caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica, potrebbe essere rivolto un ammonimento anziché imposta una sanzione pecuniaria. Si dovrebbe prestare tuttavia debita attenzione alla natura, alla gravità e alla durata della violazione, al carattere doloso della violazione e alle misure adottate per attenuare il danno subito, al grado di responsabilità o eventuali precedenti violazioni pertinenti, alla maniera in cui l'autorità di controllo ha preso conoscenza della violazione, al rispetto dei provvedimenti disposti nei confronti del titolare del trattamento o del responsabile del trattamento, all'adesione a un codice di condotta e eventuali altri fattori aggravanti o attenuanti. L'imposizione di sanzioni, comprese sanzioni amministrative pecuniarie dovrebbe essere soggetta a garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta, inclusi l'effettiva tutela giurisdizionale e il giusto processo".

[8] In alcuni paesi, in applicazione delle norme procedurali nazionali derivanti dai requisiti costituzionali, la valutazione della sanzione da infliggere può avvenire separatamente, in un momento successivo alla valutazione dell'esistenza della violazione. Ciò può limitare il contenuto e la quantità di dettagli di un progetto di decisione presentato dall'autorità di controllo capofila di tali paesi.

[9] Gli ordini, di cui all'articolo 58, paragrafo 2, sono i seguenti:
ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal regolamento;
ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del regolamento, se del caso, in una determinata maniera ed entro un determinato termine;
ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;
revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;
ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

[10] L'applicazione dell'articolo 83, paragrafo 6, deve necessariamente tenere conto del diritto procedurale nazionale. Il diritto nazionale determina le modalità di emissione e di notifica di un ordine, il momento di entrata in vigore e l'eventuale periodo di tolleranza per conformarvisi. In particolare, occorre tenere conto dell'effetto di un appello sull'esecuzione di un ordine.

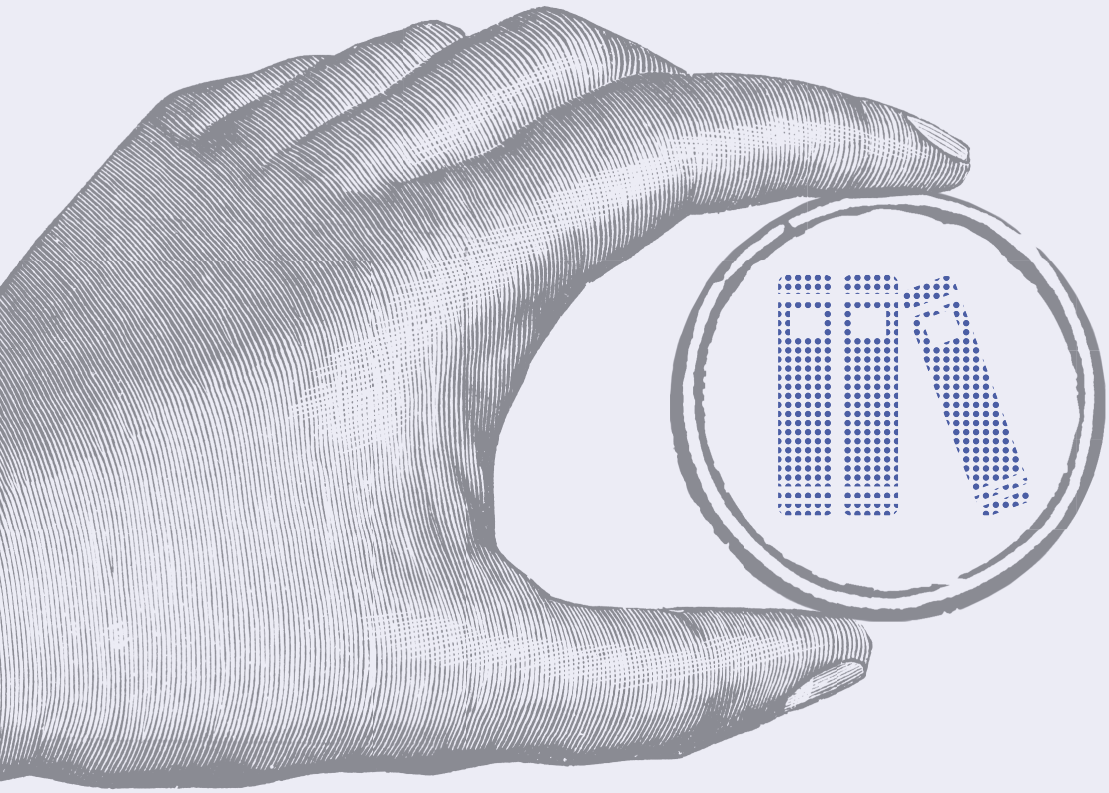
[11] Le disposizioni di legge che pongono limitazioni potrebbero far sì che un ordine precedente dell'autorità di controllo non possa più essere preso in considerazione dopo un determinato periodo dalla sua emissione. Le norme di alcune giurisdizioni prevedono che al termine del periodo di prescrizione di un ordine non possa essere imposta alcuna sanzione pecuniaria per l'inosservanza di tale ordine a norma dell'articolo 83, paragrafo 6. Spetta all'autorità di controllo di ciascuna giurisdizione determinare le ripercussioni di tali impatti.

[12] WP 203, parere 03/2013 sulla limitazione delle finalità, disponibile (in inglese) al seguente indirizzo: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[13] Vedasi anche WP 217, parere 6/2014 sul concetto di legittimo interesse del titolare del trattamento ai sensi dell'articolo 7, pagina 24, sulla questione: "Cosa rende un interesse "legittimo" o "illegittimo"?"

[14] Il fatto che la violazione riguardi solo dati indirettamente identificabili oppure pseudonimi/dati criptati non dovrebbe essere sempre considerato un fattore attenuante supplementare. Per tali violazioni una valutazione complessiva degli altri criteri potrebbe offrire una moderata o netta indicazione circa l'opportunità di imporre una sanzione amministrativa.

5 Appendice



Riferimenti utili

- **EDPB/CEPD:** Il Comitato europeo per la protezione dei dati (European Data Protection Board) è un organo europeo indipendente, che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea e promuove la cooperazione tra le Autorità competenti per la protezione dei dati dell'UE. E' composto da rappresentanti delle Autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati (GEPD). La Commissione europea e, per quanto riguarda le questioni connesse al regolamento generale sulla protezione dei dati, e l'Autorità di vigilanza EFTA hanno titolo a partecipare alle attività e alle riunioni del comitato senza diritto di voto. Sostituisce il WP29. [https://edpb.europa.eu/]
  - Linee guida, raccomandazioni e migliori prassi [https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_it]
- **EDPS/GEPD** - Garante europeo della protezione dei dati (The European Data Protection Supervisor): [https://edps.europa.eu/]. L'Autorità di controllo indipendente incaricata di vigilare sul rispetto delle norme di protezione dei dati (attualmente fissate nel Regolamento (CE) 45/2001) da parte delle istituzioni, degli organi, delle agenzie e degli organismi dell'Unione europea.
- **GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (GPDP)** – E' l'Autorità indipendente di controllo (conosciuta anche come Garante per la privacy) incaricata in Italia dell'applicazione del GDPR/RGPD, ai sensi dell'art. 2-bis del decreto legislativo 196/2003. [http://www.garanteprivacy.it/]
- **WP29**: Il Gruppo articolo 29 (Article 29 Working Party) era il gruppo di lavoro che riuniva le Autorità nazionali di vigilanza e protezione dei dati, all'interno dell'Unione europea. Era un organismo consultivo indipendente, composto da un rappresentante dalle varie Autorità nazionali, dal Garante europeo della protezione dei dati e da un rappresentante della Commissione. Traeva il suo nome dall'articolo 29 della direttiva europea 95/46. E' stato sostituito, con maggiori poteri e funzioni, dall'EDPB. [https://ec.europa.eu/newsroom/article29/news-overview.cfm]

o **Guidelines**
https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360
o **Letters and Other Documents**
https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1307

ALTRE ISTITUZIONI

- **CGUE / CURIA** - Corte di giustizia dell'Unione europea (Corte UE): [https://curia.europa.eu/]
- **DG JUST - Commissione europea** - Direzione generale giustizia e consumatori: [https://ec.europa.eu/info/departments/justice-and-consumers_it]

DAL SITO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

- **GDPR/RGPD - Regolamento europeo in materia di protezione dei dati personali:** Pagina informativa completa [https://www.garanteprivacy.it/regolamentoue]
- **Elenco delle tipologie di trattamenti soggetti al requisito di una VALUTAZIONE D'IMPATTO sulla protezione dei dati, ai sensi dell'Art. 35(4) del RGPD:** [https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9058979&zx=uvzzcc95znz3]
- **FAQ del Garante sul registro dei trattamenti:** [https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento]
- **SMEDATA:** Progetto finanziato dalla Commissione europea, cui partecipa il Garante italiano, volto a fornire alcuni strumenti pratici e interpretativi per supportare e formare i rappresentanti e gli esperti legali delle PMI (Piccole e Medie Imprese; SMEs - Small and Medium Enterprises nell'acronimo inglese), sia italiane che bulgare, nell'applicazione e negli adempimenti del RGPD. [https://www.garanteprivacy.it/regolamentoue/formazione/smedata]
- **Software PIA per la valutazione di impatto:** Software distribuito dalla CNIL (Garante Privacy francese), disponibile anche nella versione italiana curata dal Garante: [https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8581268]
- **T4Data:** Progetto finanziato dalla Commissione europea, cui partecipa il Garante italiano, che prevede attività transnazionali di formazione e iniziative formative a livello nazionale dedicate ai Responsabili della Protezione dei Dati (RPD) operanti presso i soggetti pubblici. [https://www.garanteprivacy.it/regolamentoue/formazione/t4data]
- **Tutorial su Individuazione e gestione del rischio:** [https://www.garanteprivacy.it/regolamentoue/dpia/gestione-del-rischio]

LINK EXTRA

- **EUR-Lex:** Sito ufficiale con la normativa europea [https://eur-lex.europa.eu/]
- **Privacy shield:** [https://www.privacyshield.gov/]
- **Riforma 2018 delle norme UE sulla protezione dei dati:** Pagina informativa della Commissione europea. [https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_it]

A cura del
Servizio relazioni esterne e media

Per informazioni presso l'Autorità
Ufficio per le relazioni con il pubblico
lunedì - venerdì ore 10.00 - 12.30
tel. 06 696772917
e-mail: urp@gpdp.it

Progetto grafico
Vertigo Design

Stampa
Ugo Quintily Spa – ottobre 2019

CONTRIBUTI

Le linee guida e gli altri documenti di lavoro approvati dai Garanti europei in seno all'EDPB

Il volume del Garante per la protezione dei dati personali propone tutti i documenti, in versione italiana, definitivamente approvati nel primo anno di vigenza del GDPR dal Comitato europeo per la protezione dei dati (EDPB). Il volume offre chiarimenti e spunti di riflessione a tutti coloro che, per professione o per mero interesse personale, vogliano comprendere e tutelare diritti fondamentali - come quello alla privacy e alla protezione dati – che oggi rappresentano strumenti di democrazia, prima ancora che facilitatori dell'economia contemporanea.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI