Confederazione Generale Italiana dei Trasporti e della Logistica
00198 Roma - via Panama 62 – tel.068559151-3337909556 - fax 068415576
e-mail: confetra@confetra.com - http://www.confetra.com

Roma, 4 aprile 2018

Circolare n. 73/2018

Oggetto: Ordine pubblico – Tutela della Privacy – Nuove regole dal 25 maggio – Linee Guida del Garante della Privacy.

In vista del termine del 25 maggio prossimo - data dalla quale decorrerà l'applicazione del nuovo Regolamento comunitario sulla tutela dei dati personali n.679 del 2016 – il Garante della Privacy ha redatto apposite Guide, nonché alcuni approfondimenti su temi specifici, come ad esempio la nuova figura del responsabile della protezione dei dati.

Com'è noto, la tutela della privacy non riguarda i dati delle persone giuridiche bensì esclusivamente quelli delle persone fisiche.

Rispetto alle attuali disposizioni dettate dal nostro Codice (D.Lgvo n.196/2003), le nuove disposizioni mirano a responsabilizzare ancor di più i soggetti che trattano dati personali, in particolare quelli sensibili relativi alla salute, all'origine razziale o etnica, alle opinioni politiche, all'appartenenza sindacale, al credo religioso.

Per i trattamenti di quei dati occorrerà il previo consenso dei titolari, come già avviene oggi, ma le nuove disposizioni rendono più sostanziale e meno formale la procedura di richiesta e di rilascio del consenso stesso.

Per le imprese e organizzazioni con almeno 250 dipendenti diventerà obbligatorio redigere un "Registro delle attività di trattamento" da tenere a disposizione delle autorità di controllo. La tenuta del Registro sostituirà i precedenti obblighi di notifica preventiva al Garante di determinati trattamenti.

Altra novità rilevante è la figura del Responsabile della Protezione Dati (RPD o DPO in inglese) che si affianca a quella del Titolare e del Responsabile del trattamento per fornire una consulenza costante sulla materia. L'obbligo di nominare un RPD sussiste solo per determinati trattamenti dati, come ad esempio quelli sanitari e la profilazione dei clienti persone fisiche.

In generale per i trattamenti eseguiti nell'ambito di rapporti contrattuali e di rapporti di lavoro non si rilevano novità di particolare impatto rispetto alla normativa attuale.

Pur essendo il Regolamento comunitario n.679/2016 direttamente applicabile nel nostro ordinamento, è in corso di emanazione un decreto legislativo che aggiornerà le norme nazionali attualmente in vigore.

Daniela Dringoli
Codirettore

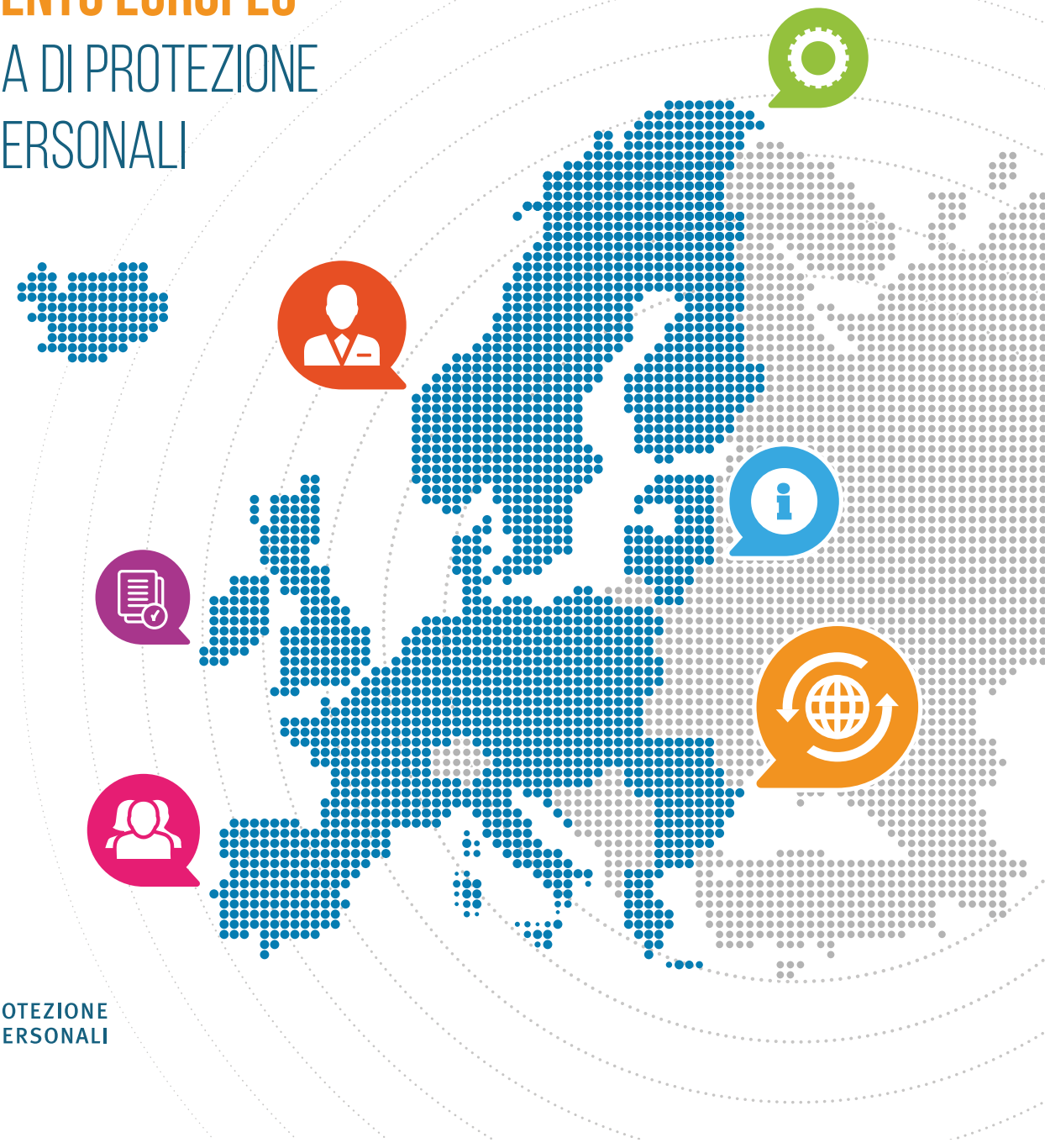
Per riferimenti confronta circ.re n.205/2017
Allegati due
D/d

© CONFETRA – La riproduzione totale o parziale è consentita esclusivamente alle organizzazioni aderenti alla Confetra.

GUIDA ALL'APPLICAZIONE DEL

REGOLAMENTO EUROPEO

IN MATERIA DI PROTEZIONE DEI DATI PERSONALI



edizione
aggiornata
febbrai0
2018

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Indice

Introduzione

La Guida intende offrire un panorama delle principali problematiche che imprese e soggetti pubblici dovranno tenere presenti in vista della piena applicazione del regolamento, prevista il 25 maggio 2018.

Attraverso raccomandazioni specifiche vengono suggerite alcune azioni che possono essere intraprese sin d'ora perché fondate su disposizioni precise del regolamento che non lasciano spazi a interventi del legislatore nazionale (come invece avviene per altre norme del regolamento, in particolare quelle che disciplinano i trattamenti per finalità di interesse pubblico ovvero in ottemperanza a obblighi di legge).

Vengono, inoltre, segnalate alcune delle principali novità introdotte dal regolamento rispetto alle quali sono suggeriti possibili approcci.

La presente Guida è soggetta a integrazioni e modifiche alla luce dell'evoluzione della riflessione a livello nazionale ed europeo

Fondamenti di liceità del trattamento

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; **i fondamenti di liceità del trattamento sono indicati all'art. 6 del regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice privacy - d.lgs. 196/2003** (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

In particolare:

Consenso

COSA CAMBIA

- Per i dati "sensibili" (si veda art. 9 regolamento) il consenso **deve** essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22). Si segnalano, al riguardo, le linee-guida in materia di profilazione e decisioni automatizzate del Gruppo "Articolo 29" (WP 251), qui disponibili: www.garanteprivacy.it/regolamentoue/profilazione.

- **Non** deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, il titolare (art. 7.1) **deve** essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

COSA NON CAMBIA

- **Il consenso dei minori** è valido **a partire dai 16 anni** (il limite di età può essere abbassato fino a 13 anni dalla normativa nazionale); prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.
- **Deve** essere, in tutti i casi, libero, specifico, informato e inequivocabile e **non** è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).
- **Deve** essere manifestato attraverso "dichiarazione o azione positiva inequivocabile" (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

Raccomandazioni

Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole continuare a fare ricorso a tale base giuridica.
In particolare, occorre verificare che la richiesta di consenso sia **chiaramente distinguibile** da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio all'interno di modulistica. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali (si vedano considerando 43, art. 9, altre disposizioni del Codice: artt. 18, 20).

Interesse vitale di un terzo

COSA CAMBIA

- Si può invocare tale base giuridica **solo** se nessuna delle altre condizioni di liceità può trovare applicazione (si veda considerando 46).

Interesse legittimo prevalente di un titolare o di un terzo

COSA CAMBIA

- Il **bilanciamento** fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato **non spetta** all'Autorità ma **è compito dello stesso titolare**; si tratta di una delle principali espressioni del principio di "responsabilizzazione" introdotto dal nuovo pacchetto protezione dati.

COSA NON CAMBIA

- L'interesse legittimo del titolare o del terzo deve prevalere sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità.
- Il regolamento chiarisce espressamente che l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.

Raccomandazioni

Il regolamento offre alcuni criteri per il bilanciamento in questione (si veda considerando 47) e soprattutto appare utile fare riferimento al documento pubblicato dal Gruppo "Articolo 29" sul punto (WP217).

Si confermano, inoltre, nella sostanza, i requisiti indicati dall'Autorità nei propri provvedimenti in materia di bilanciamento di interessi (si veda, per esempio, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680 con riguardo all'utilizzo della video-sorveglianza; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6068256 in merito all'utilizzo di sistemi di rilevazione informatica anti-frode; ecc.) con particolare riferimento agli esiti delle verifiche preliminari condotte dall'Autorità, con eccezione ovviamente delle disposizioni che il regolamento ha espressamente abrogato (per esempio: obbligo di notifica dei trattamenti). I titolari dovrebbero condurre la propria valutazione alla luce di tutti questi principi.

Informativa

Contenuti dell'informativa

COSA CAMBIA

- I contenuti dell'informativa sono elencati **in modo tassativo** negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice. In particolare, il titolare **deve sempre** specificare **i dati di contatto del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer)**, ove esistente, la **base giuridica** del trattamento, **qual è il suo interesse legittimo** se quest'ultimo costituisce la base giuridica del trattamento, nonché **se trasferisce i dati personali in Paesi terzi** e, in caso affermativo, **attraverso quali strumenti** (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).
- Il regolamento prevede anche **ulteriori informazioni** in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il **periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di **presentare un reclamo** all'autorità di controllo.
- Se il trattamento comporta processi decisionali automatizzati (anche la **profilazione**), l'informativa deve specificarlo e deve indicare anche la **logica** di tali processi decisionali e le conseguenze previste per l'interessato.

Tempi dell'informativa

COSA CAMBIA

- Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve essere fornita **entro un termine ragionevole che non può superare 1 mese** dalla raccolta, oppure **al momento della comunicazione** (**non** della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice).

Modalità dell'informativa

COSA CAMBIA

- Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**, e per i minori occorre prevedere informative idonee (si veda anche considerando 58).
- L'informativa è data, **in linea di principio, per iscritto e preferibilmente in formato elettronico** (soprattutto nel contesto di servizi online: si vedano art. 12, paragrafo 1, e considerando 58), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1). Il regolamento ammette, soprattutto, l'utilizzo di **icone** per presentare i contenuti dell'informativa in forma sintetica, **ma solo "in combinazione" con l'informativa estesa** (art. 12, paragrafo 7); queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.
- Sono inoltre **parzialmente diversi i requisiti che il regolamento fissa per l'esonero dall'informativa** (si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo), anche se occorre sottolineare che **spetta al titolare**,

COSA NON CAMBIA

in caso di dati personali raccolti da fonti diverse dall'interessato, **valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato** (si veda art. 14, paragrafo 5, lettera b)) – a differenza di quanto prevede l'art. 13, comma 5, lettera c) del Codice.

- L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del regolamento) deve essere fornita all'interessato **prima di effettuare la raccolta dei dati** (se raccolti direttamente presso l'interessato – art. 13 del regolamento). Se i dati non sono raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve comprendere anche le **categorie** dei dati personali oggetto di trattamento. In tutti i casi, il titolare deve specificare **la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati** (compreso il diritto alla portabilità dei dati), se esiste un **responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati**.

NOTA: ogni volta che le finalità cambiano il regolamento impone di informarne l'interessato prima di procedere al trattamento ulteriore.

Raccomandazioni

È opportuno che i titolari di trattamento **verifichino la rispondenza delle informative** attualmente utilizzate a tutti i criteri sopra delineati, con particolare riguardo ai **contenuti obbligatori** e alle **modalità di redazione**, in modo da apportare le modifiche o le integrazioni eventualmente necessarie ai sensi del regolamento.

Il regolamento supporta chiaramente il concetto di **informativa "stratificata"**, più volte esplicitato dal Garante nei suoi provvedimenti (si veda http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680

relativo all'utilizzo di un'icona specifica per i sistemi di videosorveglianza con o senza operatore; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1246675 contenente prescrizioni analoghe rispetto all'utilizzo associato di sistemi biometrici e di videosorveglianza in istituti bancari), in particolare attraverso l'impiego di icone associate (in vario modo) a contenuti più estesi, che devono essere facilmente accessibili, e promuove **l'utilizzo di strumenti elettronici** per garantire la massima diffusione e semplificare la prestazione delle informative.

I titolari potranno, dunque, una volta adeguata l'informativa nei termini sopra indicati, **continuare o iniziare a utilizzare queste modalità** per la prestazione dell' informativa, comprese le icone che l'Autorità ha in questi anni suggerito nei suoi provvedimenti (videosorveglianza, banche, ecc.) – in attesa della definizione di icone standardizzate da parte della Commissione.
Dovranno essere adottate anche le **misure organizzative interne** idonee a garantire il rispetto della tempistica: il termine di 1 mese per l'informativa all'interessato è chiaramente un termine massimo, e occorre ricordare che l'art. 14, paragrafo 3, lettera a), del regolamento menziona in primo luogo che il **termine deve essere "ragionevole"**.

Poiché spetterà al titolare valutare lo **sforzo sproporzionato** richiesto dall'informare una pluralità di interessati, qualora i dati non siano stati raccolti presso questi ultimi, e salva l'esistenza di specifiche disposizioni normative nei termini di cui all'art. 23, paragrafo 1, del regolamento, sarà utile fare riferimento ai **criteri evidenziati nei provvedimenti** con cui il Garante ha riconosciuto negli anni l'esistenza di tale sproporzione (si veda, in particolare, il provvedimento del 26 novembre 1998 – http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/39624; più di recente, fra molti, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3864423 in tema di esonero dagli obblighi di informativa).

Diritti degli interessati

Modalità per l'esercizio dei diritti

Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli artt. 11 e 12 del regolamento.

COSA CAMBIA

- **Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese,** estendibile fino a 3 mesi in casi di particolare complessità; **il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego**.

- **Spetta al titolare** valutare la complessità del riscontro all'interessato e **stabilire l'ammontare dell'eventuale contributo** da chiedere all'interessato, ma soltanto se si tratta di richieste **manifestamente infondate o eccessive** (anche ripetitive) (art.12, paragrafo 5), a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste **più "copie" dei dati personali** nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il **riscontro all'interessato** di regola deve avvenire in **forma scritta** anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato **oralmente solo se così richiede l'interessato** stesso (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3).

- La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche **concisa**, **trasparente e facilmente accessibile**, oltre a utilizzare un **linguaggio semplice e chiaro**.

COSA NON CAMBIA

- **Il titolare del trattamento deve agevolare l'esercizio dei diritti** da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. **Benché sia il solo titolare a dover dare riscontro** in caso di esercizio dei diritti (art. 15-22), il responsabile è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati (art. 28, paragrafo 3, lettera e)).

- **L'esercizio dei diritti è, in linea di principio, gratuito** per l'interessato, ma possono esservi eccezioni (si veda il paragrafo "Cosa cambia"). Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee (si vedano, in particolare, art. 11, paragrafo 2 e art. 12, paragrafo 6).

- Sono ammesse **deroghe ai diritti** riconosciuti dal regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonché di altri articoli relativi ad ambiti specifici (si vedano, in particolare, art. 17, paragrafo 3, per quanto riguarda il diritto alla cancellazione/"oblio", art. 83 - trattamenti di natura giornalistica e art. 89 - trattamenti per finalità di ricerca scientifica o storica o di statistica).

Raccomandazioni

È opportuno che i titolari di trattamento adottino le misure tecniche e organizzative eventualmente necessarie per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati, che – a differenza di quanto attualmente previsto – dovrà avere per impostazione predefinita forma scritta (anche elettronica). Potranno risultare utili le indicazioni fornite dal Garante nel corso degli anni con riguardo all'intelligibilità del riscontro fornito agli interessati e alla completezza del riscontro stesso (si vedano varie decisioni relative a ricorsi contenute nel Bollettino dell'Autorità pubblicato qui: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/766652, e più recentemente, fra molti, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1449401 in materia di dati sanitari, ovvero http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1290018 in materia di dati telematici).

Quanto alla definizione eventuale di un contributo spese da parte degli interessati, che il regolamento rimette al titolare del trattamento, l'Autorità intende valutare l'opportunità di definire linee-guida specifiche (anche sul fondamento delle determinazioni assunte sul punto nel corso degli anni: si veda in particolare la Deliberazione n. 14 del 23 dicembre 2004 - http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1104892), di concerto con le altre autorità Ue, alla luce di quanto prevede l'art. 70 del regolamento con riguardo ai compiti del Board.

Diritto di accesso (art. 15)

COSA CAMBIA

- Il diritto di accesso prevede **in ogni caso** il diritto di ricevere **una copia dei dati** personali oggetto di trattamento.
- Fra le informazioni che il titolare deve fornire **non rientrano le "modalità" del trattamento**, mentre **occorre indicare il periodo di conservazione** previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le **garanzie** applicate **in caso di trasferimento dei dati verso Paesi terzi**.

Raccomandazioni

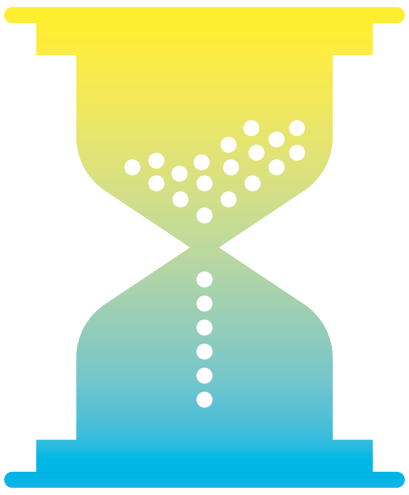
Oltre al rispetto delle prescrizioni relative alla modalità di esercizio di questo e degli altri diritti (si veda "Modalità per l'esercizio dei diritti"), i titolari possono **consentire agli interessati di consultare direttamente, da remoto** e in modo sicuro, i propri dati personali (si veda considerando 68).

Diritto di cancellazione (diritto all'oblio) (art.17)

COSA CAMBIA

- Il diritto cosiddetto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) **di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati**, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2).

- Ha **un campo di applicazione più esteso** di quello di cui all'art. 7, comma 3, lettera b), del Codice, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (si veda art. 17, paragrafo 1).



Diritto di limitazione del trattamento (art. 18)

COSA CAMBIA

- Si tratta di un diritto **diverso e più esteso rispetto al "blocco" del trattamento** di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile **non solo in caso di violazione** dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche **se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento** ai sensi dell'art. 21 del regolamento (in attesa della valutazione da parte del titolare).

- Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

Raccomandazioni

Il diritto alla limitazione prevede che **il dato personale sia "contrassegnato"** in attesa di determinazioni ulteriori; pertanto, è opportuno che i titolari prevedano nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

Diritto alla portabilità dei dati (art. 20)

COSA CAMBIA

- Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

- **Non si applica ai trattamenti non automatizzati** (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili **solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato** (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati **"forniti" dall'interessato** al titolare (si veda il considerando 68 per maggiori dettagli).

- Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

Raccomandazioni

Il Gruppo "Articolo 29" ha pubblicato recentemente linee-guida specifiche dove sono illustrati e spiegati i requisiti e le caratteristiche del diritto alla portabilità con particolare riguardo ai diritti di terzi interessati i cui dati siano potenzialmente compresi fra quelli "relativi all'interessato" di cui quest'ultimo chiede la portabilità (versione italiana con le relative FAQ qui disponibile: www.garanteprivacy.it/regolamentoue/portabilita).

Al riguardo, si ricordano i numerosi **provvedimenti con cui l'Autorità ha indicato criteri per il bilanciamento** fra i diritti e le libertà fondamentali di terzi e quelli degli interessati esercitanti i diritti di cui all'art. 7 del Codice (si vedano, fra molti, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3251012 e, con riguardo all'attività bancaria in generale, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1457247).
Poiché la trasmissione dei dati da un titolare all'altro prevede che si utilizzino formati interoperabili, i titolari che ricadono nel campo di applicazione di questo diritto dovrebbero adottare sin da ora le misure necessarie a produrre i dati richiesti in un **formato interoperabile** secondo le indicazioni fornite nel considerando 68 e nelle linee-guida del Gruppo "Articolo 29".

Titolare, responsabile, incaricato del trattamento

Il regolamento:

COSA CAMBIA

- disciplina la **contitolarità del trattamento** (art. 26) e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti **con particolare riguardo all'esercizio dei diritti degli interessati**, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente;

- fissa più dettagliatamente (rispetto al Codice) le **caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento** attribuendogli specifici compiti: deve trattarsi, infatti, di un **contratto** (o altro atto giuridico conforme al diritto nazionale) e deve **disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28** al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, e categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;

- consente la **nomina di sub-responsabili del trattamento** da parte di un responsabile (si veda art. 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo **risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile**, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo

dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (si veda art. 82, paragrafo 1 e paragrafo 3);

- prevede **obblighi specifici in capo ai responsabili del trattamento**, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la tenuta del **registro dei trattamenti** svolti (ex art. 30, paragrafo 2); l'adozione di idonee **misure tecniche e organizzative per garantire la sicurezza** dei trattamenti (ex art. 32 regolamento); **la designazione di un RPD-DPO** (si segnalano, al riguardo, le linee-guida in materia di responsabili della protezione dei dati recentemente adottate dal Gruppo "Articolo 29", qui disponibili: www.garante-privacy.it/regolamentoue/rpd), nei casi previsti dal regolamento o dal diritto nazionale (si veda art. 37 del regolamento). Si ricorda, inoltre, che **anche il responsabile** non stabilito nell'Ue dovrà **designare un rappresentante in Italia** quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del regolamento – diversamente da quanto prevedeva l'art. 5, comma 2, del Codice.

COSA NON CAMBIA

- Il regolamento definisce **caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento** negli stessi termini di cui alla direttiva 95/46/CE e, quindi, al Codice italiano. Pur non prevedendo espressamente la **figura dell' "incaricato" del trattamento** (ex art. 30 Codice), il regolamento **non ne esclude** la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (si veda, in particolare, art. 4, n. 10, del regolamento).

Raccomandazioni

I titolari di trattamento dovrebbero valutare attentamente l'esistenza di eventuali situazioni di contitolarità (si vedano, in proposito, le indicazioni fornite dal Garante in vari provvedimenti, fra cui http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/39785), essendo obbligati in tal caso a stipulare l'accordo interno di cui parla l'art. 26, paragrafo 1, del regolamento. Sarà necessario, in particolare, individuare il "punto di contatto per gli interessati" previsto dal suddetto articolo ai fini dell'esercizio dei diritti previsti dal regolamento.

I titolari di trattamento dovrebbero verificare che i contratti o altri atti giuridici che attualmente disciplinano i rapporti con i rispettivi responsabili siano conformi a quanto previsto, in particolare, dall'art. 28, paragrafo 3, del regolamento. Dovranno essere apportate le necessarie integrazioni o modifiche, in particolare qualora si intendano designare sub-responsabili nei termini sopra descritti. La Commissione e le autorità nazionali di controllo (fra cui il Garante) stanno valutando la definizione di clausole contrattuali modello da utilizzare a questo scopo.

Attraverso l'adesione a codici deontologici ovvero l'adesione a schemi di certificazione il responsabile può dimostrare le "garanzie sufficienti" di cui all'art. 28, paragrafi 1 e 4. Il Garante sta valutando i codici deontologici attualmente vigenti per alcune tipologie di trattamento nell'ottica dei requisiti fissati nel regolamento (art. 40), mentre per quanto concerne gli schemi di certificazione occorrerà attendere anche l'intervento del legislatore nazionale che dovrà stabilire alcune modalità di accreditamento dei soggetti certificatori (se diversi dal Garante: si veda art. 43).
In ogni caso, il Gruppo "Articolo 29" sta lavorando sui temi e sarà opportuno tenere conto degli sviluppi che interverranno in materia nei prossimi mesi.

Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento, in particolare alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, in tema di misure tecniche e organizzative di sicurezza, si ritiene che titolari e responsabili del trattamento possano mantenere in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante (si veda art. 30 del Codice e, fra molti, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1507921, ovvero http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1508059 per quanto riguarda la pubblica amministrazione, ovvero http://www.garante-privacy.it/web/guest/home/docweb/-/docweb-display/docweb/1813953 in materia di tracciamento delle attività bancarie) in quanto misure atte a garantire e dimostrare "che il trattamento è effettuato conformemente" al regolamento (si veda art. 24, paragrafo 1, del regolamento).

Approccio basato sul rischio e misure di accountability di titolari e responsabili

COSA CAMBIA

- Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull' **adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento** (si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento). Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

- Il primo fra tali criteri è sintetizzato dall'espressione inglese **"data protection by default and by design"** (si veda art. 25), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25, paragrafo 1 del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che **devono sostanziarsi in una serie di attività specifiche e dimostrabili.**

- Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel regolamento rispetto alla gestione degli obblighi dei titolari, ossia il **rischio inerente al trattamento**. Quest'ultimo è da intendersi come rischio

di impatti negativi sulle libertà e i diritti degli interessati (si vedano considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (si vedano artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi (si segnalano, al riguardo, le linee-guida in materia di valutazione di impatto sulla protezione dei dati del Gruppo "Articolo 29", qui disponibili: www.garanteprivacy.it/regolamentoue/DPIA). All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

- Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega **l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano**, come la **notifica preventiva dei trattamenti** all'autorità di controllo e il cosiddetto **prior checking** (o verifica preliminare: si veda art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia con eventuale successiva consultazione dell'Autorità, tranne alcune specifiche situazioni di trattamento (vedi art. 36, paragrafo 5 del regolamento). Peraltro, alle autorità di controllo, e in particolare al "Comitato europeo della protezione dei dati" (l'erede dell'attuale Gruppo "Articolo 29") spetterà un ruolo fondamenta-

le al fine di garantire uniformità di approccio e fornire ausili interpretativi e analitici: il Comitato è chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse, anche per garantire quegli adattamenti che si renderanno necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati.

Nei paragrafi seguenti si richiamano **alcune delle principali novità** in termini di adempimenti da parte di titolari e responsabili del trattamento.

Registro dei trattamenti

COSA CAMBIA

- Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Si tratta di uno **strumento fondamentale** non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – **indispensabile per ogni valutazione e analisi del rischio**. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Raccomandazioni

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì **parte integrante di un sistema di corretta gestione dei dati personali**. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata rico-

gnizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta. I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

Misure di sicurezza

COSA CAMBIA

- Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); in questo senso, **la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva** ("tra le altre, se del caso"). Per lo stesso motivo, **non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza** (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento. Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate. Tuttavia, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1, lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Notifica delle violazioni di dati personali

COSA CAMBIA

- A partire dal 25 maggio 2018, **tutti i titolari** – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, **entro 72 ore** e comunque "senza ingiustificato ritardo", ma **soltanto se ritengono probabile che da tale violazione derivino rischi** per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, **la notifica all'Autorità** dell'avvenuta violazione **non è obbligatoria**, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. **I contenuti della notifica** all'Autorità e della comunicazione agli interessati sono indicati, **in via non esclusiva, agli art. 33 e 34 del regolamento.** Si segnalano, al riguardo, le linee-guida in materia di notifica delle violazioni di dati personali del Gruppo "Articolo 29", qui disponibili: www.garanteprivacy.it/regolamentoue/databreach.

Raccomandazioni

Tutti i titolari di trattamento dovranno in ogni caso **documentare le violazioni** di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda art. 33, paragrafo 5); tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, del Codice. Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Responsabile della protezione dei dati

COSA CAMBIA

- Anche la designazione di un "responsabile della protezione dati" (RPD, ovvero DPO se si utilizza l'acronimo inglese: Data Protection Officer) riflette l'approccio responsabilizzante che è proprio del regolamento (si veda art. 39), essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare/responsabile. Non è un caso, infatti, che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'art. 35. La sua designazione è obbligatoria in alcuni casi (si veda art. 37), e il regolamento tratteggia le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali: si vedano art. 38 e 39) in termini che Gruppo "Articolo 29" ha ritenuto opportuno chiarire attraverso alcune linee-guida di recente pubblicazione, disponibili anche sul sito del Garante, e alle quali si rinvia per maggiori delucidazioni unitamente alle relative FAQ (si veda: www.garanteprivacy.it/regolamentoue/rpd).

Trasferimenti di dati verso Paesi terzi e organismi internazionali

COSA CAMBIA

- In primo luogo, **viene meno il requisito dell'autorizzazione nazionale** (si vedano art. 45, paragrafo 1, e art. 46, paragrafo 2). Ciò significa che il trasferimento verso un Paese terzo "adeguato" ai sensi della decisione assunta in futuro dalla Commissione, ovvero sulla base di clausole contrattuali modello, debitamente adottate, o di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'art. 47 del regolamento, potrà avere inizio senza attendere l'autorizzazione nazionale del Garante - a differenza di quanto attualmente previsto dall'art. 44 del Codice.
  Tuttavia, **l'autorizzazione del Garante sarà ancora necessaria** se un titolare desidera utilizzare **clausole contrattuali ad-hoc** (cioè non riconosciute come adeguate tramite decisione della Commissione europea) oppure **accordi amministrativi** stipulati tra autorità pubbliche – una delle novità introdotte dal regolamento.

- Il regolamento consente di ricorrere anche a **codici di condotta ovvero a schemi di certificazione** per dimostrare le "garanzie adeguate" previste dall'art. 46. Ciò significa che **i titolari o i responsabili del trattamento stabiliti in un Paese terzo potranno far valere gli impegni sottoscritti attraverso l'adesione al codice di condotta o allo schema di certificazione**, ove questi disciplinino anche o esclusivamente i trasferimenti di dati verso Paesi terzi, al fine di legittimare tali trasferimenti.
  Tuttavia (si vedano art. 40, paragrafo 3, e art. 42, paragrafo 2), tali titolari dovranno assumere, inoltre, **un impegno vincolante mediante uno specifico strumento contrattuale o un altro strumento** che sia giuridicamente vincolante e azionabile dagli interessati.

- Il regolamento vieta trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di **decisioni giudiziarie o ordinanze amministrative emesse da autorità di tale Paese terzo**, a meno dell'esistenza di accordi internazionali in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati (si veda art. 48). Si potranno utilizzare, tuttavia, gli altri presupposti e in particolare le deroghe previste per situazioni specifiche di cui all'art. 49. A tale riguardo, si deve ricordare che il regolamento chiarisce come sia lecito trasferire dati personali verso un Paese terzo non adeguato "per importanti motivi di interesse pubblico", in deroga al divieto generale, ma deve trattarsi di un **interesse pubblico riconosciuto dal diritto dello Stato membro** del titolare o dal diritto dell'Ue (si veda art. 49, paragrafo 4) – e dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente.

- Il regolamento **fissa i requisiti per l'approvazione delle norme vincolanti d'impresa e i contenuti obbligatori di tali norme**. L'elenco indicato al riguardo nel paragrafo 2 dell'art. 47 non è esaustivo e, pertanto, potranno essere previsti dalle autorità competenti, a seconda dei casi, requisiti ulteriori. Ad ogni modo, l'approvazione delle norme vincolanti d'impresa dovrà avvenire esclusivamente attraverso il meccanismo di coerenza di cui agli artt. 63-65 del regolamento – ossia, **è previsto in ogni caso l'intervento del Comitato europeo per la protezione dei dati** (si veda art. 64, paragrafo 1, lettera d)).

COSA NON CAMBIA

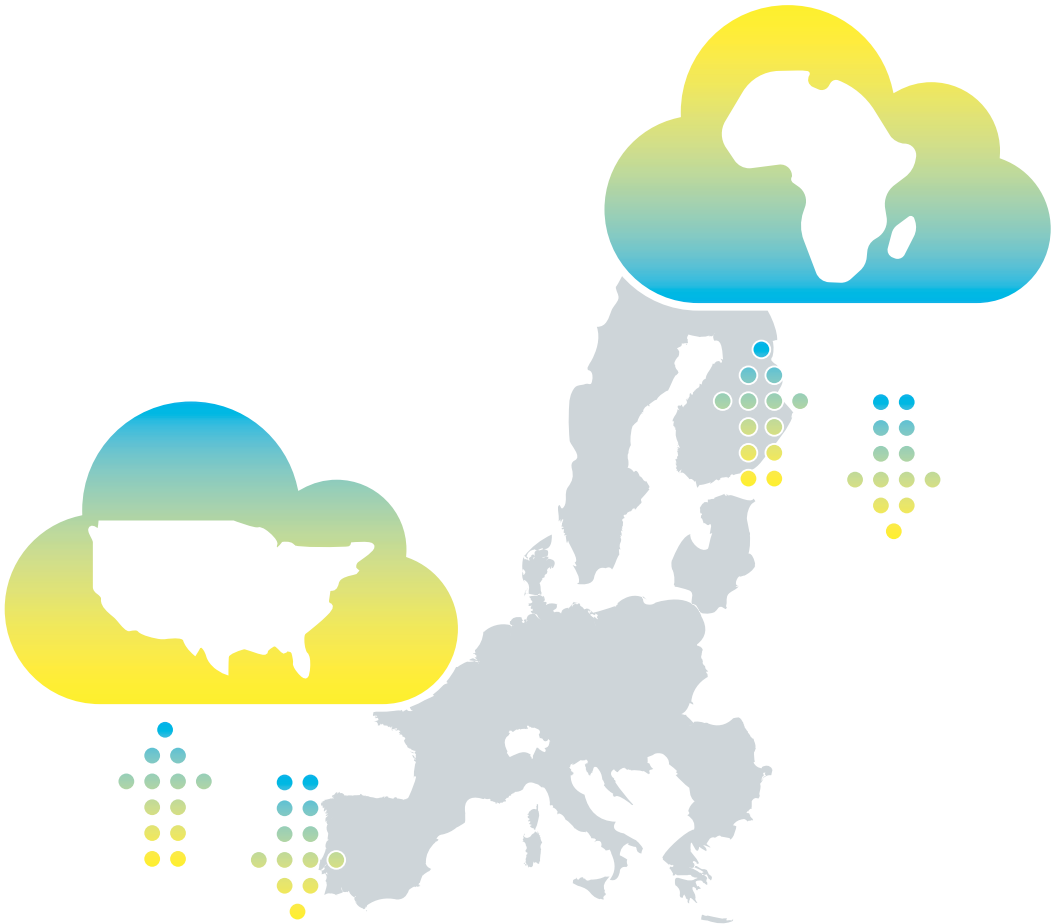
- **Il regolamento** (si veda Capo V) **ha confermato l'approccio attualmente vigente** per quanto riguarda i flussi di dati al di fuori dell'Unione europea e dello spazio economico europeo, prevedendo che tali flussi sono vietati, in linea di principio, a meno che intervengano specifiche garanzie che il regolamento elenca in ordine gerarchico:

  i. adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea;

  ii. in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa - BCR, e clausole contrattuali modello);

  iii. in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni.

- **Le decisioni di adeguatezza sinora adottate** dalla Commissione (livello di protezione dati in Paesi terzi, a partire dal Privacy Shield, e clausole contrattuali tipo per titolari e responsabili) e gli accordi internazionali in materia di trasferimento dati stipulati prima del 24 maggio 2016 dagli Stati membri restano in vigore fino a loro eventuale revisione o modifica (si vedano art. 45, paragrafo 9, e art. 96). Restano valide, conseguentemente, le autorizzazioni nazionali sinora emesse dal Garante successivamente a tali decisioni di adeguatezza della Commissione (si veda http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi#1). Restano valide, inoltre, le autorizzazioni nazionali che il Garante ha rilasciato in questi anni per specifici casi (si veda art. 46, paragrafo 5), sino a loro eventuale modifica.



Appendice

Linee guida sul regolamento gia' adottate dal gruppo di lavoro "Articolo 29" (WP29)

(Tutte le Linee guida sono disponibili sul sito internet del Garante www.garanteprivacy.it)

1. **Linee-guida sui responsabili della protezione dei dati (RPD) -** WP243
   Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016
   Comprende l'Allegato alle linee-guida sul RPD - Indicazioni essenziali

2. **Linee-guida sul diritto alla "portabilità dei dati"** - WP242
   Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016

3. **Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento** - WP244
   Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016

4. **Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679** - WP248
   Adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017

5. **Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative** - WP253
   Adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017

6. **Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e profilazione** - WP251
   Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018

7. **Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification)** - WP250
   Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VERTIGO DESIGN

Piazza di Monte Citorio, 121
00186 Roma
Tel: +39-06-696771
Fax: +39-06-696773785
www.garanteprivacy.it

Antonello Soro, Presidente
Augusta Iannini, Vice Presidente
Giovanna Bianchi Clerici, Componente
Licia Califano, Componente

Giuseppe Busia, Segretario generale

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

Pubblicazione a cura
del Servizio relazioni esterne e media

Stampa: Ugo Quintily Spa - Edizione aggiornata – febbraio 2018

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

16/IT
WP 243 rev. 01

Linee guida sui responsabili della protezione dei dati

Adottate il 13 dicembre 2016
Versione emendata e adottata in data 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

IL GRUPPO DI LAVORO SULLA TUTELA DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DI 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:

Indice

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 aumentare 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

[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

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]:

[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.

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

[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.

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.

---

[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).

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].

[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*".

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:

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.

- 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

[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.

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.

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

[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.

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 contempo, 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

[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.*"

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 collaboratori, 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

[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.

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**

[26] Capo II
[27] Capo III
[28] Articolo 25.
[29] Articolo 30.
[30] Articolo 32.
[31] Articoli 33 e 34.

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

[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.

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.

[34] Articolo 5, paragrafo 2.

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

[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".*

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.

[37] Si veda l'articolo 24, paragrafo 1, lettera d), del regolamento (CE) 45/2001.

5. 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