GRUPPO DI LAVORO ARTICOLO 29
IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

16/EN
WP 243 rev. 01

Linee-guida sui responsabili della protezione dei dati (RPD)[1]

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

Traduzione a cura del Garante per la protezione dei dati personali - Unità Documentazione Internazionale e Revisione UE

[1] **Comunemente noti con l'acronimo inglese di "DPO", ossia Data Protection Officers**

INDICE

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:

I. 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 e responsabili del trattamento sono tenuti a nominare un RPD in via obbligatoria.[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 (dati sensibili).

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" (WP29) incoraggia gli approcci di questo genere.

[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'art. 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.

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 WP29 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 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 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, primo paragrafo). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare o sul responsabile.

Inoltre, al titolare 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 a svolgere in modo efficace i compiti cui è chiamato.

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 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 WP29 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, primo paragrafo, del RGPD, la nomina di un RPD è obbligatoria in tre casi specifici:[5]

[3] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (GU L 281, 23.11.95).

[4] Si veda http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

[5] Si osservi che, in base all'art. 37, quarto paragrafo, 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 o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure

c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati[7] o[8] di dati personali relativi a condanne penali e reati[9].

In questo paragrafo, il WP29 intende fornire indicazioni rispetto ai criteri e alle formulazioni utilizzati nell'articolo 37, paragrafo 1.

Tranne quando sia evidente che un soggetto non è tenuto a nominare un RPD, il WP29 raccomanda a titolari e responsabili 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 o i responsabili intraprendono nuove attività o forniscono nuovi servizi che potrebbero ricadere nel novero dei casi elencati all'art. 37, paragrafo 1.

Se si procede alla nomina di un RPD su base volontaria, troveranno applicazione tutti i requisiti di cui agli artt. 37-39 per quanto concerne la nomina stessa, lo status e i compiti del RPD esattamente come nel caso di una nomina obbligatoria.

Nulla osta a che un'azienda o un ente, quando non sia soggetta all'obbligo di designare un RPD e non intenda procedere a tale designazione su base volontaria, ricorra comunque a personale o consulenti esterni incaricati di incombenze relative alla protezione dei dati personali. In tal caso è fondamentale garantire che non vi siano ambiguità in termini di denominazione, status e compiti di queste figure; è dunque essenziale che in tutte le comunicazioni interne all'azienda e anche in quelle esterne (con l'autorità di controllo, gli interessati, i soggetti esterni in genere), queste figure o consulenti non siano indicati con la denominazione di responsabile per la protezione dei dati (RPD).[11]

---

[6] Con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali. V. art. 32 della direttiva (Ue) 2016/680.

[7] Ai sensi dell'art. 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'art. 37, primo paragrafo, 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'art. 24, primo paragrafo.

[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".

Il RPD viene designato, su base obbligatoria o meno, per tutti i trattamenti svolti dal titolare o dal responsabile.

2.1.1. "Autorità pubblica o organismo pubblico"

Nel regolamento non si rinviene alcuna definizione di "autorità pubblica" o "organismo pubblico". Il WP29 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 WP29 raccomanda, in termini di buone prassi, che gli organismi privati incaricati di funzioni pubbliche o che esercitano pubblici poteri nominino un RPD. Le attività del RPD nominato nei termini sopra indicati si estendono a tutti i trattamenti svolti, compresi quelli che non sono connessi all'espletamento di funzioni pubbliche o all'esercizio di pubblici poteri quali, per esempio, la gestione di un database del personale.

2.1.2. "Attività principali"

L'articolo 37, paragrafo 1, lettere b) e c) del RGPD contiene un riferimento alle "*attività principali del titolare del trattamento o del responsabile del trattamento"*. Nel considerando 97 si afferma che le attività principali di un titolare del trattamento "*riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria*". Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare 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 o dal responsabile. Per esempio, l'attività principale di un ospedale consiste nella

[12] Si vedano, per esempio, le definizioni di "ente pubblico" e "organismo di diritto pubblico" contenute nell'art. 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).

prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente. Ne deriva che il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualsiasi ospedale, e che gli ospedali sono tenuti a nominare un RPD.

A titolo di ulteriore esemplificazione, si può citare il caso di un'impresa di sicurezza privata incaricata della sorveglianza di più centri commerciali e aree pubbliche. L'attività principale dell'impresa consiste nella sorveglianza, e questa, a sua volta, è legata in modo inscindibile al trattamento di dati personali. Ne consegue che anche l'impresa in oggetto deve nominare un RPD.

D'altro canto, tutti gli organismi (pubblici e privati) svolgono determinate attività quali il pagamento delle retribuzioni al personale o la predisposizione di strutture standard di supporto informatico. Si tratta di esempi di funzioni di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o essenziali sono considerate solitamente accessorie e non vengono annoverate fra le attività principali.

2.1.3. "Larga scala"

In base all'articolo 37, paragrafo 1, lettere b) e c) del RGPD, occorre che il trattamento di dati personali avvenga su larga scala per far scattare l'obbligo di nomina di un RPD. Nel regolamento non si dà alcuna definizione di trattamento su larga scala, anche se il considerando 91 fornisce indicazioni in proposito.[14]

In realtà è impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità; d'altra parte, ciò non significa che sia impossibile, col tempo, individuare alcuni standard utili a specificare in termini più specifici e/o quantitativi cosa debba intendersi per "larga scala" con riguardo ad alcune tipologie di trattamento maggiormente comuni. Anche il WP29 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 WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

[14] Il considerando in questione vi ricomprende, in particolare, "*trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato*". D'altro canto, lo stesso considerando prevede in modo specifico che "*Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato*". Si deve tener conto del fatto che il considerando offre alcune esemplificazioni ai due estremi della scala (trattamento svolto dal singolo medico / trattamento di dati relativi a un'intera nazione o a livello europeo) e che fra tali estremi si colloca un'ampia zona grigia. Inoltre, va sottolineato che il considerando citato si riferisce alle valutazioni di impatto sulla protezione dei dati; ciò significa che non tutti gli elementi citati sono necessariamente pertinenti alla nomina di un RPD negli stessi identici termini.

- 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.

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 WP29:

[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*" (art. 3, paragrafo 2, lettera b)) e "*monitoraggio regolare e sistematico degli interessati*" (art. 37, paragrafo 1, lettera b)), per cui le due espressioni potrebbero ben riferirsi a concetti distinti.

- 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 WP29:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei 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'art. 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'art. 37 non distingue fra titolari[17] e responsabili[18] del trattamento in termini di sua applicabilità. A seconda di chi soddisfi i criteri relativi all'obbligatorietà della nomina, potrà essere il solo titolare ovvero il solo responsabile, oppure sia l'uno sia l'altro a dover nominare un RPD; questi ultimi saranno poi tenuti alla reciproca collaborazione.

[17] Ai sensi della definizione contenuta all'art. 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'art. 4, punto 8, il responsabile del trattamento è la persona o l'organismo che tratta dati personali per conto del titolare del trattamento.

Vale la pena di evidenziare che anche qualora il titolare sia tenuto, in base ai criteri suddetti, a nominare un RPD, il suo eventuale responsabile del trattamento non è detto sia egualmente tenuto a procedere a tale nomina – che però può costituire una buona prassi.

Alcuni esempi:

- Una piccola azienda a conduzione familiare operante nel settore della distribuzione di elettrodomestici in una città si serve di un responsabile del trattamento la cui attività principale consiste nel fornire servizi di tracciamento degli utenti del sito web oltre all'assistenza per attività di pubblicità e marketing mirati. Le attività svolte dall'azienda e dai clienti non generano trattamenti di dati "su larga scala", in considerazione del ridotto numero di clienti e della gamma relativamente limitata di attività. Tuttavia, il responsabile del trattamento, che conta numerosi clienti come questa piccola azienda familiare, svolge, nel suo complesso, trattamenti su larga scala. Ne deriva che il responsabile deve nominare un RPD ai sensi dell'art. 37, primo paragrafo, 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 è tenuto a nominare un RPD ai sensi dell'art. 37, primo paragrafo, 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]

[19] V. art. 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. art. 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] Art. 39, paragrafo 1, lettera a).

[22] V. anche paragrafo 2.6 *infra*.

Il RPD, se necessario con il supporto di un *team* di collaboratori, deve essere in grado di comunicare con gli interessati[23] in modo efficiente e di collaborare[24] con le autorità di controllo interessate. Ciò significa, fra l'altro, che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa. Il fatto che il RPD sia raggiungibile – vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione – è fondamentale al fine di garantire all'interessato la possibilità di contattare il RPD stesso.

Ai sensi dell'articolo 37, terzo paragrafo, 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 o il responsabile 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'art. 4 [sic] del RGPD, l'accessibilità del RPD deve essere effettivamente tale. Per garantire tale accessibilità, il WP29 raccomanda che il RPD sia localizzato nel territorio dell'Unione europea, indipendentemente dal fatto che il titolare o il responsabile siano stabiliti nell'Ue.

Tuttavia, non si può escludere che, in alcuni casi ove il titolare o il responsabile 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

[23] V. art. 12, paragrafo 1: "*Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.*"
[24] V. art. 39, paragrafo 1, lettera d: "*cooperare con l'autorità di controllo.*"
[25] V. art. 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; inoltre, il RPD dovrebbe avere buona familiarità con le operazioni di trattamento svolte nonché con i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal titolare.

Nel caso di un'autorità pubblica o di un organismo pubblico, il RPD dovrebbe possedere anche una conoscenza approfondita delle norme e procedure amministrative applicabili.

- **Capacità di assolvere i propri compiti**

Per capacità di assolvere i propri compiti si deve intendere sia quanto è legato alle qualità personali e alle conoscenze del RPD, sia quanto dipende dalla posizione del RPD all'interno dell'azienda o dell'organismo. Le qualità personali dovrebbero comprendere, per esempio, l'integrità ed elevati standard deontologici; il RPD dovrebbe perseguire in via primaria l'osservanza delle disposizioni del RGPD. Il RPD svolge un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'azienda o dell'organismo, e contribuisce a dare attuazione a elementi essenziali del regolamento quali i principi fondamentali del trattamento[26], i diritti degli interessati[27], la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita[28], i registri delle attività di trattamento[29], la sicurezza dei trattamenti[30] e la notifica e comunicazione delle violazioni di dati personali.[31]

- **RPD sulla base di un contratto di servizi**

La funzione di RPD può essere esercitata anche in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna all'organismo o all'azienda titolare/responsabile del trattamento. In tal caso, è indispensabile che ciascun soggetto appartenente alla persona giuridica e operante quale RPD soddisfi tutti i requisiti applicabili come fissati nella Sezione 4

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

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 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) 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. 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 (art. 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.

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 o al responsabile 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 (art. 39, paragrafo 1, lettera e)).

[32] Si osservi che l'art. 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'art. 37, paragrafo 7, che tali informazioni comprendano anche il nominativo (e non solo le informazioni di contatto) del RPD.

In termini di buone prassi, il WP29 raccomanda, inoltre, che il titolare/responsabile 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, 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 e il responsabile 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 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. Inoltre, è importante che il RPD sia annoverato fra gli interlocutori all'interno della struttura suddetta, e che partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento.

Ciò significa che occorrerà garantire, per esempio:

- che il RPD sia invitato a partecipare su base regolare alle riunioni del management di alto e medio livello;
- la presenza del RPD ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati. Il RPD deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza idonea;
- che il parere del RPD riceva sempre la dovuta considerazione. In caso di disaccordi, il WP29 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 o il responsabile 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

[33] Art. 35, paragrafo 2.

L'articolo 38, secondo paragrafo, del RGPD obbliga il titolare o il responsabile 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, terzo paragrafo, fissa alcune garanzie essenziali per consentire ai RPD di operare con un grado sufficiente di autonomia all'interno dell'organizzazione del titolare/responsabile. 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 o il responsabile 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 o il responsabile 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'art. 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 o del responsabile. 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, terzo paragrafo, 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 o al responsabile 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.

[34] Articolo 5(2).

Le penalizzazioni possono assumere molte forme e avere natura diretta o indiretta. Per esempio, potrebbero consistere nella mancata o ritardata promozione, nel blocco delle progressioni di carriera, nella mancata concessione di incentivi rispetto ad altri dipendenti. Non è necessario che si arrivi all'effettiva applicazione di una penalizzazione, essendo sufficiente anche la sola minaccia nella misura in cui sia rivolta al RPD in rapporto alle attività da questi svolte.

Viceversa, e conformemente alle normali regole di gestione applicabili a ogni altro dipendente o fornitore soggetto alla disciplina del rispettivo contratto nazionale ovvero alle norme di diritto penale e del lavoro, sarebbe legittimamente possibile interrompere il rapporto con il RPD per motivazioni diverse dallo svolgimento dei compiti che gli sono propri: per esempio, in caso di furto, molestie sessuali o di altro genere, o altre analoghe e gravi violazioni deontologiche.

In questo ambito va rilevato che il RGPD non specifica le modalità e la tempistica riferite alla cessazione del rapporto di lavoro del RPD o alla sua sostituzione. Tuttavia, quanto maggiore è la stabilità del contratto stipulato con il RPD e maggiori le tutele previste contro l'ingiusto licenziamento, tanto maggiore sarà la probabilità che l'azione del RPD si svolga in modo indipendente. Il WP29 vede, quindi, con favore ogni iniziativa assunta in tal senso dai titolari e responsabili di trattamento.

3.5. Conflitto di interessi

In base all'art. 38, paragrafo 6, al RPD è consentito di "*svolgere altri compiti e funzioni*", ma a condizione che il titolare 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 o del responsabile, 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 o responsabile.

A grandi linee, possono sussistere situazioni di conflitto all'interno dell'organizzazione del titolare o del responsabile 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 o del responsabile, 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'art. 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 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*" (art. 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'art. 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'art. 35, secondo paragrafo, prevede in modo specifico che il titolare "*si consulta*" con il RPD quando svolge una DPIA. A sua volta, l'art. 39, primo paragrafo, 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 WP29 raccomanda che il titolare 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 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 WP29 raccomanda che il titolare 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'art. 39, paragrafo 1, lettere d) ed e), il RPD deve "cooperare con l'autorità di controllo" e "fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione".

Questi compiti attengono al ruolo di "facilitatore" attribuito al RPD e già menzionato nell'introduzione alle presenti Linee-guida. Il RPD funge da punto di contatto per facilitare l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei compiti attribuitile dall'art. 57 nonché ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi di cui all'art. 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 (art. 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'art. 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

[35] I compiti del RPD sono elencati all'art. 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'art. 39, paragrafo 1, ovvero di specificare ulteriormente i suddetti compiti.

[36] L'art. 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"*.

In base all'art. 39, secondo paragrafo, 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'art. 30, primo e secondo paragrafo, prevede che sia il titolare 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'art. 39, primo paragrafo, contiene un elenco non esaustivo dei compiti affidati al RPD. Pertanto, niente vieta al titolare 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 o del responsabile.

In ogni caso, il registro la cui tenuta è obbligatoria ai sensi dell'art. 30 deve essere considerato anche uno strumento che consente al titolare 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'art. 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 o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
- se le attività principali del titolare o del responsabile 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" (WP29) 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 o dal responsabile del trattamento, comprese tutte quelle attività per le quali il trattamento dei dati è inscindibilmente connesso all'attività del titolare o del responsabile. 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: art. 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 WP29 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: art. 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 WP29:

- 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 WP29:

- 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*: *art. 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 o il responsabile 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: art. 37, paragrafi 2) e 3), RGPD

6. Dove dovrebbe collocarsi il RPD?

Per garantire l'accessibilità del RPD, il WP29 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 o responsabile 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 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: art. 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: art. 37, paragrafo 5, RGPD

Posizione del RPD

9. Quali sono le risorse che titolare o responsabile 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 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 in modo da ricevere tutto il supporto, le informazioni o gli input necessari;
- formazione permanente.

Fonte: art. 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 o del responsabile 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 o del responsabile, 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 o responsabile.

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 o il responsabile in un giudizio che tocchi problematiche di protezione dei dati.

Fonte: art. 38, paragrafi 3 e 6, RGPD

Compiti del RPD

11. Che cosa si intende per "sorvegliare l'osservanza"

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, e
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

Fonte: art. 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 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 / 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 o il responsabile 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.

In merito al registro dei trattamenti, la sua tenuta è un obbligo che ricade sul titolare o sul responsabile, e non sul RPD. Cionondimeno, niente vieta al titolare 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 o del responsabile.

Fonte: art. 39, paragrafo 1, lettera c) e art. 30, RGPD

Bruxelles, 13 dicembre 2016

Per il Gruppo di lavoro
La presidente

Isabelle FALQUE-PIERROTIN

Versione emendata e adottata in data 5 aprile 2017