

WP243 ALLEGATO – DOMANDE FREQUENTI

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 responsabile della protezione dei dati (articolo 37)

1 Chi è tenuto a designare un RPD? (articolo 37, paragrafo 1)

La designazione di un RPD è obbligatoria in tre casi specifici:

- 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;
- 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.

Per maggiori informazioni si veda la sezione 2.1 delle linee guida.

2 Cosa significa "attività principali"? (articolo 37, paragrafo 1, lettere b) e c))

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.

Per maggiori informazioni si veda la sezione 2.1.2 delle linee guida.

3 Cosa significa "su larga scala"? (articolo 37, paragrafo 1, lettere b) e c))

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.

Per maggiori informazioni si veda la sezione 2.1.3 delle linee guida.

4 Cosa significa “monitoraggio regolare e sistematico”? (articolo 37, paragrafo 1, lettera b))

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.

Secondo il Gruppo di lavoro l'aggettivo “regolare” ha almeno uno dei seguenti significati:

- 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.

Secondo il Gruppo di lavoro, 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.

Esempi: 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.

Per maggiori informazioni si veda la sezione 2.1.4 delle linee guida.

5 E' ammessa la designazione congiunta di uno stesso RPD da parte di più soggetti? A quali condizioni? (articolo 37, paragrafi 2 e 3)

In base al RGPD 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.

Per maggiori informazioni si veda la sezione 2.3 delle linee guida.

6 Si può designare un RPD esterno (articolo 37, paragrafo 6)?

Sì. In base all'articolo 37, paragrafo 6, 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.

Al RPD esterno si applicano tutti i requisiti di cui agli articoli da 37 a 39. Come esposto nelle linee guida, se la funzione di RPD è svolta da un fornitore esterno di servizi, i compiti stabiliti per il RPD potranno essere assolti efficacemente da un team operante sotto l'autorità di un contatto principale designato e *“responsabile”* per il singolo cliente. In 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, 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.

Per maggiori informazioni si vedano le sezioni 2.3, 2.4 e 3.5 delle linee guida.

7 Quali sono le qualità professionali che un RPD deve possedere (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 [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.

Per maggiori informazioni si veda la sezione 2.4 delle linee guida.

Posizione del RPD (articolo 38)

8 Quali sono le risorse che dovrebbero essere messe a disposizione del RPD per lo svolgimento dei suoi compiti?

Ai sensi dell'articolo 38, paragrafo 2, del RGPD "il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti [...] fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica".

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.

Per maggiori informazioni si veda la sezione 3.2 delle linee guida.

9 Quali sono le garanzie che possono consentire al RPD di operare con indipendenza (articolo 38, paragrafo 3)?

Come indicato al considerando 97 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.

Per maggiori informazioni si vedano le sezioni da 3.3 a 3.5 delle linee guida.

10 Quali sono gli “altri compiti e funzioni” del RPD che possono dare adito a un conflitto di interessi (articolo 38, paragrafo 6)?

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.

Per maggiori informazioni si veda la sezione 3.5 delle linee guida.

Compiti del RPD (articolo 39)

11 Quali compiti rientrano nella nozione di "sorvegliare l'osservanza" (articolo 39, paragrafo 1, lettera b)?

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.

Per maggiori informazioni si veda la sezione 4.1 delle linee guida.

12 Il RPD è personalmente responsabile in caso di inosservanza del RGPD?

No, il RPD non è responsabile personalmente in caso di inosservanza del RGPD. Quest'ultimo dispone chiaramente che 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. (articolo 24, paragrafo 1). 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 (articolo 37, paragrafo 1, lettera c)) e alla tenuta del registro dei trattamenti (articolo 30)?

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 al RGPD.

Per maggiori informazioni si veda la sezione 4.2 delle linee guida.

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.

Per maggiori informazioni si veda la sezione 4.4 delle linee guida.