PRIVACY

“Privacy”: il responsabile della sicurezza dei dati personali

Tutte le FAQ su nomina, requisiti, compiti e responsabilità del responsabile della protezione dati

di Armando Urbano | 11 APRILE 2018

L’art. 37 del Reg. CE 27 aprile 2016, n. 2016/679/UE, ha previsto la figura del responsabile dei dati personali (*data protection officer*) per assolvere ad alcune specifiche funzioni, quali: sorvegliare l’osservanza del regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell’ambito di applicazione, del contesto e delle finalità; collaborare con il titolare/responsabile nel condurre una valutazione di impatto sulla protezione dei dati (DPIA); informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati; cooperare con il Garante e fungere da punto di contatto per il medesimo su ogni questione connessa al trattamento e supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali.
Vista la particolarità della figura, il Garante per la protezione dei dati personali ha ritenuto opportuno pubblicare sul proprio sito le FAQ sul responsabile della protezione dei dati (RPD), sia in ambito pubblico che in ambito privato, in aggiunta a quelle adottate dal Gruppo Art. 29 (WP29), in allegato alle Linee guida sull’RPD.
Ricordiamo che si svolge oggi a Milano il Convegno gratuito “Gli adempimenti privacy dello studio professionale”, il Convegno verrà riproposto domani a Cagliari e il 19 aprile a Roma.

SOMMARIO:

Premessa

Il Regolamento della Comunità europea 27 aprile 2016, n. 2016/679/UE, pubblicato sulla *Gazzetta Ufficiale dell’Unione europea* n. L 119 del 4 maggio 2016, concernente la tutela delle persone fisiche con riguardo al **trattamento dei dati personali** e la libera circolazione di tali dati, è entrato **in vigore il 24 maggio 2016** (ventesimo giorno successivo alla pubblicazione sulla *Gazzetta ufficiale dell’Unione europea*), ma, in base all’art. 99 dello stesso regolamento “*esso* ***si applica a decorrere dal 25 maggio 2018***”.

Per chiarire meglio le norme del regolamento il Gruppo di lavoro Art. 29 per la protezione dei dati (WP29) ha predisposto apposite **Linee guida**, che sono pubblicate sul sito del Garante per la protezione dei dati personali sul sito: www.garanteprivacy.it.

Il **gruppo di lavoro** è stato istituito in virtù dell’art. 29 della Dir. CEE 24 ottobre 1995, n. 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’art. 30 della Dir. n. 95/46/CE e all’art. 15 della Dir. CEE 12 luglio 2002, n. 2002/58/CE.

Attenzione

Tra le novità introdotte dal regolamento vi è la figura del responsabile dei dati personali e i soggetti obbligati dovranno **dotarsi, entro il 25 maggio 2018, di questo esperto in materia di trattamento dei dati personali**.

Il responsabile della protezione dei dati

L'art. 37 del Reg. UE n. 2016/679, nonchè la motivazione di cui al Considerando 97 dello stesso regolamento, hanno previsto la figura del responsabile della protezione dei dati (RPD), conosciuto anche con la dizione inglese *data protection officer* (DPO), che è un **organo indipendente**, coinvolto in tutte le questioni attinenti alla *privacy*, la cui **nomina è obbligatoria in alcuni specifici casi**.

Obbligo di nomina del DPO

Devono designare obbligatoriamente un RPD:

1. **Amministrazioni ed enti pubblici**, fatta eccezione per le autorità giudiziarie.

Esempio

Sono Amministrazioni ed enti pubblici:
- le Amministrazioni dello Stato, anche con ordinamento autonomo;
- gli enti pubblici non economici nazionali, regionali e locali;
- le regioni e gli enti locali;le università;
- le Camere di commercio, industria, artigianato e agricoltura;
- le aziende del Servizio sanitario nazionale;
- le autorità indipendenti, ecc.

Attenzione

Il Gruppo di lavoro raccomanda, in termini di buone prassi, che gli **organismi privati, incaricati di funzioni pubbliche o che esercitano pubblici poteri** (ad esempio, concessionari di servizi pubblici), per i quali non sussista l'obbligo di nominare un RPD, lo designino comunque.

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 gli RPD designati in via obbligatoria;

2. tutti i soggetti la cui **attività principale** consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala**;

3. tutti i soggetti la cui **attività principale** consiste nel **trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici**.

Attenzione

Le Linee guide emanate il 13 dicembre 2016, successivamente emendate e adottate il 5 aprile 2017, dal Gruppo di lavoro Art. 29, al fine di **stabilire se un trattamento sia effettuato su larga scala**, raccomandano di tenere conto, in particolare, dei seguenti fattori:
- 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.

Esempio

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 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.

Il Gruppo di lavoro Art. 29, nelle proprie Linee guida, ha voluto precisare cosa deve intendersi per il monitoraggio regolare e sistematico.

La nozione di **monitoraggio** ricomprende senza dubbio tutte le forme di **tracciamento e profilazione su *internet***, anche per finalità di pubblicità comportamentale, ma non trova applicazione solo con riguardo all'ambiente *online*, in quanto il tracciamento *online* va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati.

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.

Esempio

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.

Anche per i casi in cui il regolamento non impone in modo specifico la designazione di un RPD è comunque possibile una **nomina su base volontaria**.

Attenzione

Ai sensi dell'art. 37, par. 2, un **gruppo di imprese** o soggetti pubblici può nominare un **unico RPD**, a **condizione** che quest'ultimo sia "*facilmente raggiungibile da ciascuno stabilimento*".

I requisiti del DPO

Il responsabile della protezione dei dati, nominato dal titolare del trattamento o dal responsabile del trattamento, deve:

1. possedere un'**adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. **Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali**, anche se la **partecipazione a *master* e corsi di studio/professionali** può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze.
2. adempiere alle sue funzioni in piena **indipendenza** e in **assenza di conflitti di interesse**. In linea di principio, ciò significa che l'RPD non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali;
3. operare alle **dipendenze del titolare o del responsabile** oppure sulla base di un **contratto di servizio** (RPD/DPO esterno).

Al titolare del trattamento o al responsabile del trattamento spetta il compito fondamentale di consentire lo svolgimento efficace dei compiti cui l'RPD è preposto. La nomina di un RPD è solo il primo passo, perché l'RPD deve disporre anche di autonomia e risorse sufficienti per svolgere in modo efficace i propri compiti.

⚠ Attenzione

Pertanto, il **titolare o il responsabile del trattamento** dovranno **mettere a disposizione** del responsabile della protezione dei dati le **risorse umane e finanziarie** necessarie all'adempimento dei suoi compiti.

I compiti del DPO

1. **Sorvegliare l'osservanza del regolamento**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
2. **collaborare con il titolare/responsabile**, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);
3. **informare e sensibilizzare** il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
4. **cooperare con il Garante** e fungere da punto di contatto per il medesimo su ogni questione connessa al trattamento e per questo motivo il suo **nominativo va comunicato al Garante**;
5. **supportare il titolare o il responsabile** in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento.

Responsabilità del DPO

I responsabili per la protezione dei dati **non rispondono personalmente** in caso di inosservanza del Reg. n. 2016/679/UE (RGPD), in quanto 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.

⚠ Attenzione

L'**onere** di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul **titolare del trattamento o sul responsabile del trattamento**.

Nuove "FAQ" sul responsabile della protezione dei dati in ambito privato

Il 26 marzo 2018 il Garante per la protezione dei dati personali, per chiarire alcuni dubbi in merito alla nomina, ai requisiti e alla designazione del responsabile della protezione dei dati (RPD), ha pubblicatosul proprio sito le FAQ (*frequently asked questions*) che interessano tale figura in ambito privato, in aggiunta a quelle adottate dal Gruppo Art. 29 (WP29), in allegato alle Linee guida sull'RPD.

Il Garante aveva pubblicato il 15 dicembre 2017, sempre sul proprio sito, le FAQ relative al responsabile della protezione dei dati in **ambito pubblico**.

Di seguito si riportano le FAQ complete relative al DPO in **ambito privato**.

1. Chi è il responsabile della protezione dei dati personali (RPD) e quali sono i suoi compiti?

Il responsabile della protezione dei dati personali (anche conosciuto con la dizione in lingua inglese *data protection officer - DPO*) è una figura prevista dall'art. 37 del Reg. (UE) n. 2016/679. Si tratta di un soggetto designato dal titolare o dal responsabile del trattamento per assolvere a **funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del regolamento** medesimo. **Coopera con l'autorità** (e proprio per questo, il suo nominativo va comunicato al Garante; v. FAQ 6) e costituisce il **punto di contatto**, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (artt. 38 e 39 del regolamento).

2. Quali requisiti deve possedere il responsabile della protezione dei dati personali?

Il responsabile della protezione dei dati personali, al quale non sono richieste specifiche attestazioni formali

o l'iscrizione in appositi albi, deve possedere un'**approfondita conoscenza della normativa e delle prassi in materia di *privacy*, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento**.

Deve potere offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per **progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali**, coadiuvando il titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Deve inoltre agire in piena **indipendenza** (considerando 97 del Reg. UE n. 2016/679) e **autonomia**, senza ricevere istruzioni e riferendo direttamente ai vertici.

Il responsabile della protezione dei dati personali deve potere **disporre**, infine, di **risorse** (personale, locali, attrezzature, ecc.) **necessarie per l'espletamento dei propri compiti**.

3. Chi sono i soggetti privati obbligati alla sua designazione?

Sono tenuti alla designazione del responsabile della protezione dei dati personali il titolare e il responsabile del trattamento che rientrino nei casi previsti dall'art. 37, par. 1, lett. b) e c), del Reg. (UE) n. 2016/679. Si tratta di soggetti le cui **principali attività** (*in primis*, le attività cd. di "*core business*") consistono in trattamenti che richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali o di dati relative a condanne penali e a reati** (per quanto attiene alle nozioni di "monitoraggio regolare e sistematico" e di "larga scala", v. le "Linee guida sui responsabili della protezione dei dati" del 5 aprile 2017, WP 243). Il diritto dell'Unione o degli Stati membri può prevedere ulteriori casi di designazione obbligatoria del responsabile della protezione dei dati (art. 37, par. 4).

Esempio

Ricorrendo i suddetti presupposti, sono tenuti alla nomina, a titolo esemplificativo e non esaustivo:
- istituti di credito;
- imprese assicurative;
- sistemi di informazione creditizia;
- società finanziarie;
- società di informazioni commerciali;
- società di revisione contabile;
- società di recupero crediti;
- istituti di vigilanza;partiti e movimenti politici;sindacati;CAF e patronati;
- società operanti nel settore delle "*utilities*" (telecomunicazioni, distribuzione di energiaelettrica o gas);
- imprese di somministrazione di lavoro e ricerca del personale;
- società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali - ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione;
- società di *call center*;
- società che forniscono servizi informatici;
- società che erogano servizi televisivi a pagamento.

4. Chi sono i soggetti per i quali non è obbligatoria la designazione del responsabile della protezione dei dati personali?

Nei casi diversi da quelli previsti dall'art. 37, par. 1, lett. b) e c), del Reg. (UE) n. 2016/679, la designazione del responsabile del trattamento non è obbligatoria.

Esempio

In relazione a trattamenti effettuati da:
- liberi professionisti operanti in forma individuale;
- agenti, rappresentanti e mediatori operanti non su larga scala;
- imprese individuali o familiari;
- piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti: v. anche considerando 97 del regolamento, in relazione alla definizione di attività "accessoria".

In ogni caso, resta comunque **raccomandata**, anche alla luce del principio di "***accountability***" che permea il regolamento, la **designazione** di tale figura (v., in proposito, le menzionate Linee guida), i cui criteri di nomina, in tale evenienza, rimangono gli stessi sopra indicati.

5. È possibile nominare un unico responsabile della protezione dei dati personali nell'ambito di un gruppo imprenditoriale?

Il Reg. (UE) n. 2016/679 (rego2016042700679) prevede che un **gruppo** imprenditoriale (v. definizione di cui all'art. 4 , n. 19) **possa designare un unico responsabile** della protezione dei dati personali, **purché** tale responsabile sia **facilmente raggiungibile da ciascuno stabilimento** (sul concetto di "raggiungibilità", v. punto 2.3 delle Linee guida in precedenza menzionate).

⚠ Attenzione

Inoltre, dovrà essere in grado di comunicare in modo efficace con gli interessati e di collaborare con le autorità di controllo.

6. Il responsabile della protezione dei dati personali deve essere un soggetto interno o può essere anche un soggetto esterno? Quali sono le modalità per la sua designazione?

Il ruolo di responsabile della protezione dei dati personali può essere ricoperto da un **dipendente del titolare o del responsabile** (non in conflitto di interessi) che conosca la realtà operativa in cui avvengono i trattamenti; l'incarico può essere anche affidato a **soggetti esterni, a condizione che garantiscano l'effettivo assolvimento dei compiti** che il Reg. (UE) n. 2016/679 (rego2016042700679) assegna a tale figura. Il responsabile della protezione dei dati **scelto all'interno** andrà nominato mediante specifico **atto di designazione**, mentre quello **scelto all'esterno**, che dovrà avere le medesime prerogative e tutele di quello interno, dovrà operare in base a un **contratto di servizi**. Tali atti, da redigere in **forma scritta**, dovranno **indicare espressamente**:

- i compiti attribuiti;
- le risorse assegnate per il loro svolgimento;
- ogni altra utile informazione in rapporto al contesto di riferimento.

Nell'esecuzione dei propri compiti, il responsabile della protezione dei dati personali (interno o esterno) dovrà ricevere **supporto adeguato** in termini di risorse finanziarie, infrastrutturali e, ove opportuno, di personale. Il titolare o il responsabile del trattamento che abbia designato un responsabile per la protezione dei dati personali resta comunque pienamente responsabile dell'osservanza della normativa in materia di protezione dei dati e deve essere in grado di dimostrarla (art. 5, par. 2, del regolamento; v. anche i punti 3.2 e 3.3. delle Linee guida sopra richiamate).

I **dati di contatto** del responsabile designato dovranno essere infine **pubblicati** dal titolare o responsabile del trattamento. **Non è necessario** - anche se potrebbe rappresentare una buona prassi - **pubblicare anche il nominativo** del responsabile della protezione dei dati: spetta al titolare o al responsabile e allo stesso responsabile della protezione dei dati valutare se, in base alle specifiche circostanze, possa trattarsi di un'informazione utile o necessaria.

⚠ Attenzione

Il **nominativo** del responsabile della protezione dei dati e i relativi **dati di contatto** vanno invece **comunicati all'autorità di controllo**.

A tale fine, allo stato, è possibile utilizzare il modello di cui al seguente *link*: http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/7322292.

7. Il ruolo di responsabile della protezione dei dati personali è compatibile con altri incarichi?

Si, a condizione che **non sia in conflitto di interessi**. In tale prospettiva, appare preferibile **evitare** di assegnare il ruolo di responsabile della protezione dei dati personali a **soggetti con incarichi di alta direzione** (amministratore delegato; membro del consiglio di amministrazione; direttore generale; ecc.), ovvero nell'ambito di **strutture aventi potere decisionale in ordine alle finalità e alle modalità del trattamento** (direzione risorse umane, direzione *marketing*, direzione finanziaria, responsabile IT, ecc.). **Da valutare**, in assenza di conflitti di interesse e in base al contesto di riferimento, l'eventuale assegnazione di tale incarico ai **responsabili delle funzioni di *staff*** (ad esempio, il responsabile della funzione legale).

8. Il responsabile della protezione dei dati personali è una persona fisica o può essere anche un soggetto diverso?

Il Reg. (UE) n. 2016/679 (rego2016042700679) prevede espressamente che il responsabile della protezione dei dati personali possa essere un "dipendente" del titolare o del responsabile del trattamento (art. 37, par. 6, del regolamento); ovviamente, nelle realtà organizzative di medie e grandi dimensioni, il responsabile della protezione dei dati personali, **da individuarsi comunque in una persona fisica**, potrà essere **supportato**

anche da un apposito ufficio, dotato delle competenze necessarie ai fini dell'assolvimento dei propri compiti.

Qualora il responsabile della protezione dei dati personali sia individuato in un **soggetto esterno**, quest'ultimo **potrà essere anche una persona giuridica** (v. il punto 2.4 delle suddette Linee guida).

Attenzione

Si raccomanda, in ogni caso, di procedere a una **chiara ripartizione di competenze**, individuando **una sola persona fisica** atta a fungere da **punto di contatto** con gli interessati e l'autorità di controllo.

Riferimenti normativi:

- Regolamento della Comunità europea 27 aprile 2016, n. 2016/679/UE.

Argomenti trattati

PRIVACY **TRATTAMENTO DEI DATI PERSONALI** **TITOLARE DEL TRATTAMENTO DEI DATI** **RESPONSABILE DEL TRATTAMENTO DEI DATI** **RESPONSABILE DELLA PROTEZIONE DEI DATI**