PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 19 - numero 4149 di Lunedì 8 gennaio 2018

Le nuove faq sul Responsabile della Protezione dei dati

Pubblicate sul sito del Garante per la protezione dei dati personali nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico.

Sul sito del Garante per la protezione dei dati personali, un'autorità amministrativa istituita dalla cosiddetta legge sulla privacy (legge 31 dicembre 1996, n. 675) e oggi disciplinata dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003 n. 196), sono state pubblicate nuove ***Faq sul Responsabile della Protezione dei dati*** *(RPD) in ambito pubblico, in aggiunta a quelle adottate dal Gruppo Art. 29 (Gruppo di lavoro articolo 29 in materia di protezione dei dati personali) e con riferimento al Regolamento generale sulla protezione dei dati (RGPD).*

1. Quali sono i soggetti tenuti alla designazione del RPD, ai sensi dell'art. 37, par. 1, lett. a), del RGPD?

L'art. 37, par. 1, lett. a), del RGPD prevede che i titolari e i responsabili del trattamento designino un RPD «quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali».

Il RGPD non fornisce la definizione di "autorità pubblica" o "organismo pubblico" e, come chiarito anche nelle Linee guida adottate in materia dal Gruppo Art. 29 (di seguito Linee guida), ne rimette l'individuazione al diritto nazionale applicabile (1).

Allo stato, in ambito pubblico, devono ritenersi tenuti alla designazione di un RPD i soggetti che oggi ricadono nell'ambito di applicazione degli artt. 18 - 22 del Codice, che stabiliscono le regole generali per i trattamenti effettuati dai soggetti pubblici (ad esempio, le amministrazioni dello Stato, anche con ordinamento autonomo, gli enti pubblici non economici nazionali, regionali e locali, le Regioni e gli enti locali, le università, le Camere di commercio, industria, artigianato e agricoltura, le aziende del Servizio sanitario nazionale, le autorità indipendenti ecc.).

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0143] ?#>

Occorre, comunque, considerare che, nel caso in cui soggetti privati esercitino funzioni pubbliche (in qualità, ad esempio, di concessionari di servizi pubblici), può risultare comunque fortemente raccomandato, ancorché non obbligatorio, procedere alla designazione di un RPD. In ogni caso, qualora si proceda alla designazione di un RPD su base volontaria, si applicano gli identici requisiti - in termini di criteri per la designazione, posizione e compiti - che valgono per i RPD designati in via obbligatoria (2).

2. Nel caso in cui il RPD sia un dipendente dell'autorità pubblica o dell'organismo pubblico, quale qualifica deve avere?

Il RGPD non fornisce specifiche indicazioni al riguardo. È opportuno, in primo luogo, valutare se il complesso dei compiti assegnati al RPD - aventi rilevanza interna (consulenza, pareri, sorveglianza sul rispetto delle disposizioni) ed esterna (cooperazione con l'autorità di controllo e contatto con gli interessati in relazione all'esercizio dei propri diritti) - siano (o meno) compatibili con le mansioni ordinariamente affidate ai dipendenti con qualifica non dirigenziale.

In merito, l'art. 38, par. 3, del RGPD fissa alcune garanzie essenziali per consentire ai RPD di operare con un grado sufficiente di autonomia all'interno dell'organizzazione. In particolare, occorre assicurare che il RPD "non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti". Il considerando 97 aggiunge che i RPD "dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente". Ciò significa, come chiarito nelle Linee guida, che «il RPD, nell'esecuzione dei compiti attribuitigli ai sensi dell'articolo 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico ? quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo. Né deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati».

Inoltre, sempre ai sensi dell'art. 38, par. 3, del RGPD, il RPD «riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento». Tale rapporto diretto garantisce, in particolare, che il vertice amministrativo venga a conoscenza delle indicazioni e delle raccomandazioni fornite dal RPD nell'esercizio delle funzioni di informazione e consulenza a favore del titolare o del responsabile.

Alla luce delle considerazioni di cui sopra, nel caso in cui si opti per un RPD interno, sarebbe quindi in linea di massima preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, la designazione sia conferita a un dirigente ovvero a un funzionario di alta professionalità, che possa svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione.

3. Quali certificazioni risultano idonee a legittimare il RPD nell'esercizio delle sue funzioni, ai sensi degli artt. 42 e 43 del RGPD?

Come accade nei settori delle cosiddette "professioni non regolamentate", si sono diffusi schemi proprietari di certificazione volontaria delle competenze professionali effettuate da appositi enti certificatori. Tali certificazioni (che non rientrano tra quelle disciplinate dall'art. 42 del RGPD) sono rilasciate anche all'esito della partecipazione ad attività formative e al controllo dell'apprendimento.

Esse, pur rappresentando, al pari di altri titoli, un valido strumento ai fini della verifica del possesso di un livello minimo di conoscenza della disciplina, tuttavia non equivalgono, di per sé, a una "abilitazione" allo svolgimento del ruolo del RPD né, allo stato, sono idonee a sostituire il giudizio rimesso alle PP.AA. nella valutazione dei requisiti necessari al RPD per svolgere i compiti previsti dall'art. 39 del RGPD (3).

4. Con quale atto formale deve essere designato il RPD?

Il RGPD prevede all'art. 37, par. 1, che il titolare e il responsabile del trattamento designino il RPD; da ciò deriva, quindi, che l'atto di designazione è parte costitutiva dell'adempimento.

Nel caso in cui la scelta del RPD ricada su una professionalità interna all'ente, occorre formalizzare un apposito atto di designazione a "Responsabile per la protezione dei dati". In caso, invece, di ricorso a soggetti esterni all'ente, la designazione costituirà parte integrante dell'apposito contratto di servizi redatto in base a quanto previsto dall'art. 37 del RGPD (4) (per agevolare gli enti, in allegato alle Faq, è riportato uno schema di atto di designazione).

Indipendentemente dalla natura e dalla forma dell'atto utilizzato, è necessario che nello stesso sia individuato in maniera inequivocabile il soggetto che opererà come RPD, riportandone espressamente le generalità (5), i compiti (eventualmente anche ulteriori a quelli previsti dall'art. 39 del RGPD (6)) e le funzioni che questi sarà chiamato a svolgere in ausilio al titolare/responsabile del trattamento, in conformità a quanto previsto dal quadro normativo di riferimento.

L'eventuale assegnazione di compiti aggiuntivi, rispetto a quelli originariamente previsti nell'atto di designazione, dovrà comportare la modifica e/o l'integrazione dello stesso o delle clausole contrattuali.

Nell'atto di designazione o nel contratto di servizi devono risultare succintamente indicate anche le motivazioni che hanno indotto l'ente a individuare, nella persona fisica selezionata, il proprio RPD, al fine di consentire la verifica del rispetto dei requisiti previsti dall'art. 37, par. 5 del RGPD, anche mediante rinvio agli esiti delle procedure di selezione interna o esterna effettuata. La specificazione dei criteri utilizzati nella valutazione compiuta dall'ente nella scelta di tale figura, oltre a essere indice di trasparenza e di buon amministrazione, costituisce anche elemento di valutazione del rispetto del principio di «responsabilizzazione».

Una volta individuato, il titolare o il responsabile del trattamento è tenuto a indicare, nell'informativa fornita agli interessati, i dati di contatto del RPD pubblicando gli stessi anche sui siti web e a comunicarli al Garante (art. 37, par. 7). Per quanto attiene al sito web, può risultare opportuno inserire i riferimenti del RPD nella sezione "amministrazione trasparente", oltre che nella sezione "privacy" eventualmente già presente.

Come chiarito nelle Linee guida, in base all'art. 37, par. 7, non è necessario -anche se potrebbe costituire una buona prassi, in ambito pubblico- pubblicare anche il nominativo del RPD, mentre occorre che sia comunicato al Garante per agevolare i contatti con l'Autorità (anche in questo caso, in allegato alle Faq, è riportato un modello di comunicazione al Garante). Resta invece fermo l'obbligo di comunicare il nominativo agli interessati in caso di violazione dei dati personali (art. 33, par. 3, lett. b) (7).

5. La designazione di un RPD interno all'autorità pubblica o all'organismo pubblico richiede necessariamente anche la costituzione di un apposito ufficio?

Il RGPD prevede, all'art. 38, par. 2, che «il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica».

Ne discende che, in relazione alla complessità (amministrativa e tecnologica) dei trattamenti e dell'organizzazione, occorrerà valutare attentamente se una sola persona possa essere sufficiente a svolgere il complesso dei compiti affidati al RPD. Come riportato anche nelle Linee guida, «in linea di principio, quanto più aumentano complessità e/o sensibilità dei trattamenti, tanto maggiori devono essere le risorse messe a disposizione del RPD. La funzione "protezione dati" deve poter operare con efficienza e contare su risorse sufficienti in proporzione al trattamento svolto».(8)

All'esito di questa analisi si potrà valutare quindi l'opportunità/necessità di istituire un apposito ufficio al quale destinare le risorse necessarie allo svolgimento dei compiti stabiliti. Ad ogni modo, ove sia costituito un apposito ufficio, è comunque necessario che venga sempre individuata la persona fisica che riveste il ruolo di RPD (mediante l'atto di designazione di cui sopra).(9)

6. È ammissibile che uno stesso titolare/responsabile del trattamento abbia più di un RPD?

Alcune organizzazioni complesse hanno richiesto all'Autorità di valutare la possibilità di designare più RPD.

Al riguardo, si rileva che l'unicità della figura del RPD è una condizione necessaria per evitare il rischio di sovrapposizioni o incertezze sulle responsabilità, sia con riferimento all'ambito interno all'ente, sia con riferimento a quello esterno, e pertanto occorre che questa sia sempre assicurata.

Nulla osta, invece, all'individuazione di più figure di supporto, con riferimento a settori o ambiti territoriali diversi, anche dislocate presso diverse articolazioni organizzative dell'amministrazione, che facciano però riferimento a un unico soggetto responsabile, sia che la scelta ricada su un RPD interno, sia che questa ricada su un RPD esterno.

Infatti, in relazione alla particolare eterogeneità dei trattamenti di dati personali effettuati (in rapporto, ad esempio, all'effettuazione di trattamenti soggetti a basi giuridiche diverse in ambito di prevenzione, indagine, accertamento e perseguimento di reati) ovvero della complessità della struttura organizzativa dell'ente (talvolta molto ramificata a livello territoriale) può risultare opportuno individuare specifici "referenti" del RPD che potrebbero svolgere un ruolo di supporto e raccordo, sulla base di precise istruzioni del RPD, anche, se del caso, operando quali componenti del suo gruppo di lavoro.(10)

7. Quali sono gli ulteriori compiti e funzioni che possono essere assegnati a un RPD?

Il RGPD consente l'assegnazione al RPD di ulteriori compiti e funzioni, a condizione che non diano adito a un conflitto di interessi (art. 38, par. 6e che consentano al RPD di avere a disposizione il tempo sufficiente per l'espletamento dei compiti previsti dal RGPD (art. 38, par. 2).

A seconda della natura dei trattamenti e delle attività e dimensioni della struttura del titolare o del responsabile, le eventuali ulteriori incombenze attribuite al RPD non dovrebbero pertanto sottrarre allo stesso il tempo necessario per adempiere alle relative responsabilità.

In linea di principio, è quindi ragionevole che negli enti pubblici di grandi dimensioni, con trattamenti di dati personali di particolare complessità e sensibilità, non vengano assegnate al RPD ulteriori responsabilità (si pensi, ad esempio, alle amministrazioni centrali, alle agenzie, agli istituti previdenziali, nonché alle regioni e alle asl). In tale quadro, ad esempio, avuto riguardo, caso per caso, alla specifica struttura organizzativa, alla dimensione e alle attività del singolo titolare o responsabile, l'attribuzione delle funzioni di RPD al responsabile per la prevenzione della corruzione e per la trasparenza, considerata la molteplicità degli adempimenti che incombono su tale figura, potrebbe rischiare di creare un cumulo di impegni tali da incidere negativamente sull'effettività dello svolgimento dei compiti che il RGPD attribuisce al RPD.

Rispetto all'assenza di conflitto di interessi, occorre inoltre valutare se, come indicato nelle Linee guida, le eventuali ulteriori funzioni assegnate non comportino la definizione di finalità e modalità del trattamento dei dati. Ciò significa che, a grandi linee, in ambito pubblico, oltre ai ruoli manageriali di vertice, possono sussistere situazioni di conflitto di interesse rispetto a figure apicali dell'amministrazione investite di capacità decisionali in ordine alle finalità e ai mezzi del trattamento di dati personali posto in essere dall'ente pubblico, ivi compreso, ad esempio, il responsabile dei Sistemi informativi (chiamato ad individuare le misure di sicurezza necessarie), ovvero quello dell'Ufficio di statistica (deputato a definire le caratteristiche e le metodologie del trattamento dei dati personali utilizzati a fini statistici).

Riguardo agli ulteriori compiti e funzioni in capo al RPD, particolare attenzione andrebbe infine prestata nei casi di unico RPD tra molteplici autorità pubbliche e organismi pubblici, nonché nei casi di RPD esterno, in quanto questi potrebbe svolgere ulteriori compiti che comportano situazioni di conflitto di interesse oppure non essere in grado di adempiere in modo efficiente alle sue funzioni. In questi casi, nell'atto di designazione o nel contratto di servizio il RPD dovrà fornire opportune garanzie per favorire efficienza e correttezza e prevenire conflitti di interesse.

NOTE

(1) Cfr. al riguardo il par. 2.1.1., pag. 6, delle Linee guida sui responsabili della protezione dei dati (RPD) adottate dal Gruppo Art. 29 il 13 dicembre 2016 ed emendate il 5 aprile 2017 (WP243 rev. 01), disponibili sul sito istituzionale dell'Autorità (doc. web n. 5930287).

(2) Anche in caso di assenza del requisito soggettivo previsto dall'art. 37, par. 1, lett. a), del RGPD, il titolare o il responsabile del trattamento sono comunque tenuti alla designazione del RPD, ai sensi di quanto previsto dall'art. 37, par. 1, lett. b) e c), nel caso in cui le attività principali consistano:

- in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala;

- nel trattamento su larga scala di categorie di dati personali di cui all'art. 9 del RGPD o dei dati relativi alle condanne penali e a reati di cui all'art. 10 del RGPD.

Con riferimento all'interpretazione delle espressioni «attività principali», «larga scala» e «monitoraggio regolare e sistematico» vedasi quanto riportato nelle Linee guida.

(3) Sul tema della certificazione inoltre si richiama l'attenzione sul comunicato congiunto, pubblicato sul sito dell'Autorità il 18 luglio 2017 (doc. web n. 6621723), con il quale il Garante e ACCREDIA (l'Ente unico nazionale di accreditamento designato dal Governo italiano) hanno ritenuto necessario sottolineare - al fine di indirizzare correttamente le attività svolte dai soggetti a vario titolo interessati in questo ambito - che «al momento le certificazioni di persone, nonché quelle emesse in materia di privacy o data protection eventualmente rilasciate in Italia, sebbene possano costituire una garanzia e atto di diligenza verso le parti interessate dell'adozione volontaria di un sistema di analisi e controllo dei principi e delle norme di riferimento, a legislazione vigente non possono definirsi "conformi agli artt. 42 e 43 del regolamento 2016/679", poiché devono ancora essere determinati i "requisiti aggiuntivi" ai fini dell'accreditamento degli organismi di certificazione e i criteri specifici di certificazione».

(4) Al riguardo, si ricorda che la funzione di RPD può essere esercitata anche in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna al titolare/responsabile del trattamento. In tal caso, come indicato nelle citate Linee guida, è indispensabile che ciascun soggetto appartenente alla persona giuridica operante quale RPD soddisfi tutti i requisiti richiesti dal RGPD. Cfr. sul punto le indicazioni del Gruppo Art. 29 riportate nel paragrafo 2.5., pag. 12, e nella domanda n. 7, pag. 24, delle Linee guida.

(5) Secondo quanto precisato nelle Linee guida, se la funzione di RPD è svolta da un fornitore esterno di servizi, i compiti stabiliti per il RPD potranno essere assolti efficacemente da un team operante sotto l'autorità di un contatto principale designato e "responsabile" per il singolo cliente. In particolare, «per favorire una corretta e trasparente organizzazione interna e prevenire conflitti di interesse a carico dei componenti il team RPD, si raccomanda di procedere a una chiara ripartizione dei compiti all'interno del team RPD e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente. Sarà utile, in via generale, inserire specifiche disposizioni in merito nel contratto di servizi» (cfr. par. 2.5., pag. 12).

(6) Cfr. la Faq n. 7 in relazione alla preliminare valutazione sulla compatibilità di ulteriori compiti e funzioni da assegnare al RPD.

(7) Cfr. al riguardo il paragrafo 2.6. delle Linee guida.

(8) Vedi sul punto Linee guida, paragrafo 3.2., pag. 15.

(9) Cfr., in proposito, la nota n. 4.

(10) In caso di RPD esterno, cfr. le note nn. 4 e 5.

Fonte: Garante per la protezione dei dati personali

Scarica i documenti citati:

Linee-guida sui responsabili della protezione dei dati (RPD) - WP 243 (formato PDF, 424 kB);

Schema di atto di designazione del Responsabile della Protezione dei Dati personali (RDP) ai sensi dell'art 37 del Regolamento UE 2016/679 (formato DOC, 43 kB);

Modello comunicazione al Garante dei dati dell'RPD ai sensi dell'art 37, par 1, lett a) e par 7, del RGPD (formato DOC, 34 kB);

Regolamento Ue e certificazione in materia di dati personali(formato PDF, 100 kB).

Scarica la normativa:

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)

Questo articolo è pubblicato sotto una Licenza Creative Commons.

www.puntosicuro.it