PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4943 di Giovedì 27 maggio 2021

Linee di indirizzo e FAQ del Garante privacy per gli RPD

Indicazione del Garante su designazione, posizione e compiti del Responsabile protezione dei dati (Rpd) in ambito pubblico e le FAQ per l'ambito privato.

Qual è il ruolo effettivo del Responsabile della protezione dati nella Pa? Quali titoli e che tipo di esperienza professionale deve possedere? Quando è incompatibile con altri incarichi o può incorrere in situazioni di conflitto di interessi? Come deve essere supportato e coinvolto, e per quali compiti?

A queste e a molte altre domande risponde il Garante per la privacy con un documento di indirizzo su designazione, posizione e compiti del Responsabile protezione dei dati (Rpd) in ambito pubblico, sul sito www.gpdp.it.

Garante Privacy - Provvedimento del 29 aprile 2021 - Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico

L'esigenza di fornire chiarimenti si è resa necessaria perché, a distanza di tre anni dalla piena applicazione del Regolamento Ue, si registrano ancora diverse incertezze che impediscono la definitiva affermazione di questa importante figura, obbligatoria per il settore pubblico.

Il Rpd costituisce un riferimento essenziale per garantire un corretto approccio al trattamento dei dati, soprattutto ora che le Pa sono sempre più sollecitate dalla sfida della "trasformazione digitale".

Un Rpd esperto e competente, in grado di svolgere i propri compiti con autonomia di giudizio e indipendenza, rappresenta infatti, anche nell'attuale periodo di emergenza sanitaria, una risorsa fondamentale per le amministrazioni e un valido punto di contatto per l'Autorità.

Il documento di indirizzo, in corso di pubblicazione nella Gazzetta ufficiale, sarà inviato ai vertici delle amministrazioni nazionali e territoriali e alle realtà rappresentative del mondo pubblico, affinché ne favoriscano la più ampia diffusione.

Oltre al documento rivolto alla Pa, il Garante è intervenuto aggiornando le Faq riguardanti il settore privato. Anche in questo ambito il Rdp, pur presentando sensibili differenze rispetto al mondo delle pubbliche amministrazioni, svolge un ruolo fondamentale. Si tratta infatti di una figura chiamata ad assolvere funzioni di supporto, di controllo, consultive e formative, che deve essere adeguatamente coinvolta in tutte le attività che riguardano la protezione dei dati in azienda.

Anche le Faq aggiornate sono disponibili da oggi sul sito dell'Autorità.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[CODE] ?#>

Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato

(in aggiunta a quelle adottate dal Gruppo Art. 29 in Allegato alle Linee guida sul RPD)

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

Il responsabile della protezione dei dati personali (di seguito "RPD"; o anche conosciuto come Data protection officer) è una figura prevista dall'art. 37 del Regolamento (UE) 2016/679 (di seguito "RGPD"). Si tratta di un soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e di controllo, consultive, formative e informative relativamente all'applicazione del RGPD. A tal fine, deve essere "tempestivamente e adeguatamente" coinvolto in tutte le questioni riguardanti la protezione dei dati personali anche con riferimento ad attività di interlocuzione con l'Autorità (quali, ad esempio, audizioni, accertamenti ispettivi o riunioni svolte a vario titolo; cfr. art. 38, par. 1 del RGPD). Coopera, inoltre, con l'Autorità e costituisce il punto di contatto rispetto a quest'ultima e agli interessati, in merito alle questioni connesse al trattamento dei dati personali (artt. 38 e 39 del RGPD).

Parole chiave: funzioni, punto di contatto.

Riferimenti normativi: art. 37, 38 e 39, RGPD; c. 97, RGPD.

Approfondimenti: Gruppo ex art. 29, Linee guida sui responsabili della protezione dei dati, del 5 aprile 2017 ? WP 243 rev. 01; provv. del Garante del 17 dicembre 2020 ? doc. web n. 9524175.

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

Il RPD, 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 protezione dei dati personali, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento.

Deve poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema di gestione dei dati personali, coadiuvando il titolare o il responsabile del trattamento nell'adozione di un complesso di misure organizzative (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Deve inoltre agire in piena indipendenza (considerando 97 del RGPD) e autonomia, senza ricevere istruzioni in ordine all'esecuzione dei menzionati compiti e riferendo direttamente ai vertici del titolare o del responsabile del trattamento (art. 38, par. 3 del RGPD).

Il responsabile della protezione dei dati personali deve poter disporre, infine, di risorse (personale, locali, attrezzature, ecc.) necessarie per l'espletamento dei propri compiti (art. 38, par. 2 del RGPD).

Parole chiave: attestazione, albo, indipendenza, autonomia, istruzioni, risorse.

Riferimenti normativi: art. 37, par. 5 e art. 38, paragrafi 2 e 3, RGPD; c. 97, RGPD.

Approfondimenti: Gruppo ex art. 29, Linee guida sui responsabili della protezione dei dati, del 5 aprile 2017 ? WP 243 rev. 01, paragrafi 2.5, 3.2 e 3.3.

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

Sono tenuti alla designazione del RPD il titolare o il responsabile del trattamento che rientrino nei casi previsti dall'art. 37, par. 1, lettere b) e c), del RGPD. Si tratta di soggetti le cui principali attività (in primis, le attività c.d. 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. Gruppo ex art. 29, "Linee guida sui responsabili della protezione dei

dati" del 5 aprile 2017, WP 243 rev. 01 , paragrafi 2.1.3 e 2.1.4) [inserire link al relativo documento]. Il diritto dell'Unione o degli Stati membri può prevedere ulteriori casi di designazione obbligatoria del RPD (art. 37, par. 4 del RGPD; cfr., in tal senso, ad esempio, art. 2-sexiesdecies del D. lgs. 196/2003).

Ricorrendo i suddetti presupposti, sono tenuti alla nomina, a titolo esemplificativo e non esaustivo: concessionari di servizi pubblici (trasporto pubblico locale, raccolta dei rifiuti, gestione dei servizi idrici ecc.), 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 energia elettrica o gas, ecc.); 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.

Parole chiave: designazione, attività principale, larga scala, monitoraggio.

Riferimenti normativi: art. 37, par. 1, lettere b) e c) e art. 37, par. 4, RGPD; c. 97, RGPD; art. 2-sexiesdecies, D. lgs. 196/2003.

Approfondimenti: Gruppo ex art. 29, Linee guida sui responsabili della protezione dei dati, del 5 aprile 2017 ? WP 243 rev. 01, paragrafi 2.1 e 2.2.

4. Per quali categorie di soggetti la designazione del RPD non è obbligatoria ma comunque opportuna?

Nei casi diversi da quelli previsti dall'art. 37, par. 1, lettere b) e c), del RGPD, la designazione del RPD non è obbligatoria (ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale o comunque che non effettuano trattamenti su larga scala; amministratori di condominio; agenti, rappresentanti e mediatori non operanti 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 - a tale ultimo riguardo, cfr. anche considerando 97 del RGPD, in relazione alla definizione di attività "accessoria").

In ogni caso, resta comunque raccomandata, anche alla luce del principio di accountability che permea il RGPD, la designazione di tale figura (v., in proposito, WP 243, cit., par. 1), i cui criteri di nomina, in tale evenienza, rimangono gli stessi sopra indicati.

Parole chiave: designazione, piccole e medie imprese, attività accessoria.

Riferimenti normativi: art. 37, par. 1, RGPD; c. 97, RGPD.

Approfondimenti: Gruppo ex art. 29, Linee guida sui responsabili della protezione dei dati, del 5 aprile 2017 ? WP 243 rev. 01, paragrafi 1, 2.1, 2.1.2 e 2.1.3.

5. Il RPD deve essere un soggetto interno o può essere anche un soggetto esterno? Quali sono le modalità per la sua designazione?

Il ruolo di RPD 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. In entrambi i casi, i soggetti designati devono essere in grado di garantire l'effettivo assolvimento dei compiti che il RGPD assegna a tale figura. Il RPD scelto all'interno andrà nominato mediante specifico atto di designazione (ad es. lettera d'incarico), mentre quello scelto all'esterno, che dovrà avere le medesime prerogative e tutele di quello interno, dovrà operare in base a un contratto (cfr. art. 37, par. 6 del RGPD, ove si fa riferimento al "contratto di servizi"). Tali atti, da redigere in forma scritta, dovranno contenere la designazione del RPD e indicare espressamente i compiti ad esso attribuiti, le risorse assegnate per il loro svolgimento, nonché

ogni altra utile informazione in rapporto al contesto di riferimento.

Nell'esecuzione dei propri compiti, il RPD (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 mantengono comunque la piena responsabilità in ordine all'osservanza della normativa in materia di protezione dei dati.

Parole chiave: dipendente, soggetto esterno, contratto, atto, designazione.

Riferimenti normativi: artt. 37 e 38, RGPD; c. 97, RGPD.

Approfondimenti: Gruppo ex art. 29, Linee guida sui responsabili della protezione dei dati, del 5 aprile 2017 ? WP 243 rev. 01, paragrafi 2.5, 3.2 e 3.3.

6. Il RPD deve essere nominato responsabile del trattamento?

No. Il RPD, in ragione dell'autonomia d'azione specificatamente attribuita al medesimo dalla normativa (artt. 38 e 39 del RGPD), non può essere nominato responsabile del trattamento, figura quest'ultima distinta ed espressamente disciplinata dall'art. 28 del RGPD.

Parole chiave: responsabile del trattamento, nomina.

Riferimenti normativi: artt. 28, 38 e 39, RGPD; c. 81 e 97, RGPD.

Approfondimenti: Gruppo ex art. 29, Linee guida sui responsabili della protezione dei dati, del 5 aprile 2017 ? WP 243 rev. 01; EDPB, "Guidelines 07/2020 on the concepts of controller and processor in the GDPR", del 2 settembre 2020.

7. Quali sono gli ulteriori adempimenti che il titolare o il responsabile deve porre in essere in occasione della designazione del RPD?

Il titolare o il responsabile del trattamento è tenuto a pubblicare i dati di contatto del RPD designato e a comunicarli al Garante (art. 37, par. 7 del RGPD).

Non è necessario pubblicare il nominativo del RPD, purché i relativi dati di contatto consentano che lo stesso sia direttamente e agevolmente raggiungibile (ad es. per il tramite di un indirizzo e-mail a ciò dedicato).

Il nominativo del responsabile della protezione dei dati e i relativi dati di contatto vanno invece comunicati all'Autorità di controllo tramite una procedura telematica ad hoc [inserire link al modulo https://servizi.gpdp.it/comunicazionerpd/s/], provvedendo, con le medesime modalità, al loro tempestivo aggiornamento in caso di modifica dei predetti dati o di sostituzione del soggetto designato.

Tale procedura rappresenta l'unico canale di contatto utilizzabile a questo specifico fine; maggiori informazioni in merito sono reperibili alla pagina https://www.gpdp.it/regolamentoue/rpd#PROCEDURA, ove sono riportate le apposite istruzioni e le relative FAQ.

Parole chiave: dati di contatto, nominativo, comunicazione.

Riferimenti normativi: art. 37, par. 7, RGPD; art. 39, par. 1, lett. e), RGPD.

Approfondimenti: Gruppo ex art. 29, Linee guida sui responsabili della protezione dei dati, del 5 aprile 2017 ? WP 243 rev. 01, par. 2.6; modulo di comunicazione predisposto dal Garante, reperibile al seguente link https://servizi.gpdp.it/comunicazionerpd/s/; FAQ inerenti alla procedura telematica per la comunicazione dei dati del RPD,

reperibili al seguente link
https://www.gpdp.it/regolamentoue/rpd/faq-relative-alla-procedura-telematica-per-la-comunicazione-dei-dati

8. Il ruolo di RPD è compatibile con altri incarichi?

Si, a condizione che non sia in conflitto di interessi.

In tale prospettiva, ove il RPD sia individuato in un soggetto interno all'organizzazione, appare incompatibile l'assegnazione del ruolo di RPD a soggetti con incarichi di alta direzione o aventi specifiche funzioni (es. amministratore delegato; membro del consiglio di amministrazione; direttore generale; responsabile IT, responsabile audit e/o gestione del rischio, responsabile del servizio prevenzione e protezione ecc.), ovvero nell'ambito di strutture aventi potere decisionale in ordine alle finalità e alle modalità del trattamento (es. direzione risorse umane, direzione marketing, direzione finanziaria, ecc.). Pertanto, potrebbe essere valutata l'assegnazione di tale incarico ai responsabili delle funzioni di staff (ad esempio, il responsabile della funzione legale), previa verifica, in base al contesto di riferimento, circa l'assenza di conflitto di interessi.

Laddove il RPD sia una figura esterna all'organizzazione, non appare compatibile con i requisiti di indipendenza previsti dall'art. 38 del RGPD, l'assegnazione di tale incarico a soggetti che, nel rendere servizi nell'interesse del titolare, potrebbero trovarsi in una posizione di conflitto di interessi (es. fornitore di servizi IT, software-house, ecc.).

Parole chiave: conflitto d'interessi, funzioni, mansioni, soggetto esterno, incarico.

Riferimenti normativi: art. 38, paragrafi 3 e 6, RGPD; c. 97, RGPD.

Approfondimenti: Gruppo ex art. 29, Linee guida sui responsabili della protezione dei dati, del 5 aprile 2017 ? WP 243 rev. 01, par. 3.5.

9. Il RPD è una persona fisica o può essere anche un soggetto diverso?

Il RGPD prevede espressamente che il RPD possa essere un "dipendente" del titolare o del responsabile del trattamento (art. 37, par. 6, del Regolamento) in grado di svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione.

Il RPD, inoltre, 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 RPD sia individuato in un soggetto esterno, quest'ultimo potrà essere anche una persona giuridica (v. WP 243, par. 2.5), purché sia indicata la persona fisica atta a fungere da punto di contatto con gli interessati e con l'Autorità di controllo.

Al fine di agevolare il soggetto esterno che opera come RPD, sarebbe altresì opportuno individuare all'interno dell'organizzazione del titolare o del responsabile, una figura, che funga da referente per il RPD.

Parole chiave: dipendente, soggetto esterno, persona fisica, persona giuridica.

Riferimenti normativi: art. 37, par. 6 e art. 38, par. 2, RGPD; c. 97, RGPD.

Approfondimenti: Gruppo ex art. 29, Linee guida sui responsabili della protezione dei dati, del 5 aprile 2017 ? WP 243 rev. 01, par. 2.5.

10. È possibile nominare un unico RPD nell'ambito di un gruppo imprenditoriale?

Il RGPD prevede che un gruppo imprenditoriale (v. definizione di cui all'art. 4, n. 19 del RGPD) possa designare un unico RPD, purché tale responsabile sia facilmente raggiungibile da ciascuno stabilimento (sul concetto di "raggiungibilità", v. WP 243, par. 2.3). Inoltre, dovrà essere in grado di comunicare in modo efficace con gli interessati e di collaborare con le Autorità di controllo.

A tal fine, potrebbe essere buona prassi nei gruppi di impresa, quella di prevedere che il RPD di gruppo sia assistito da specifici referenti locali individuati presso ciascuna entità (anche, se del caso, operando quali componenti del suo gruppo di lavoro), in grado di fornire adeguato supporto allo stesso e di fungere da punto di contatto nei confronti dei soggetti interessati e dell'Autorità di controllo competente; ciò, ad esempio, al fine di coadiuvare a livello locale la gestione dei reclami degli interessati e l'attività di formazione del personale; veicolare le principali questioni emerse in materia di protezione dei dati personali nelle singole entità del gruppo, ecc.

Viceversa, ove non si opti per un unico RPD ma, all'interno del gruppo imprenditoriale, vengano nominati singoli RPD per ciascuna entità, al fine di assicurare un efficace coordinamento dei compiti loro assegnati, potrebbe essere valutata l'opportunità di costituire un network dei medesimi, individuando, se del caso, anche una figura di riferimento (ad es. il RPD della società capogruppo) con funzioni volte a garantire un adeguato raccordo tra gli stessi (ad es. per il tramite di riunioni periodiche; scambio di informazioni ecc.).

Resta in tutti i casi fermo, come già evidenziato in termini generali nella faq n. 7, l'obbligo, in capo alle singole entità del gruppo in qualità di titolari o responsabili del trattamento, di pubblicare i dati di contatto del RPD e di comunicarli all'Autorità di controllo competente.

Parole chiave: gruppo di imprese, referente, network.

Riferimenti normativi: art. 4, n. 19, RGPD; art. 37, par. 2, RGPD; c. 97, RGPD.

Approfondimenti: Gruppo ex art. 29, Linee guida sui responsabili della protezione dei dati, del 5 aprile 2017 ? WP 243 rev. 01, par. 2.3; Gruppo ex art. 29, "Documento di lavoro che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa", WP 256 rev.01, del 6 febbraio 2018, par. 2.4; Gruppo ex art. 29, WP 257 rev. 01, "Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules", del 6 febbraio 2018, par. 2.4.

Garante Privacy - Provvedimento del 29 aprile 2021 - Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico

Fonte: Garante Privacy

Questo articolo è pubblicato sotto una Licenza Creative Commons.

www.puntosicuro.it