IL RUOLO DEL RESPONSABILE DELLA PROTEZIONE DATI

Sommario

Sommario 1
Disclaimer 1
1. Obbligatorietà della nomina del RPD nella PA 2
2. Competenze del RPD 4
3. Posizionamento del RPD nell'ambito dell'organizzazione e conflitti di interesse 5
3.1. Autonomia e indipendenza 5
3.2. Competenze del RPD 6
3.3. Rapporti con altri ruoli interni 7
4. Compiti e funzioni del RPD 8
4.1. Compiti tipici (obbligatori) 8
4.2. Compiti ulteriori (facoltativi) 10
5. Modalità di coinvolgimento del RPD e sua *accountability* 11

Disclaimer

Questo documento rappresenta le opinioni e le interpretazioni degli Autori, presenti all'interno del Network dei Responsabili della Protezione Dati (RPD) delle Autorità amministrative indipendenti, e non rappresenta il punto di vista dei rispettivi enti di appartenenza, né li vincola sotto alcun profilo. Gli Autori, le Autorità amministrative indipendenti e gli altri membri del Network non sono in alcun modo responsabili di qualsivoglia uso delle informazioni qui contenute.

Premessa

Il presente documento intende fornire dei parametri interpretativi di base per individuare e istituire correttamente la figura del Responsabile della Protezione dei Dati (di seguito: RPD), introdotta nel nostro ordinamento dal Regolamento (UE) 2016/679, Regolamento Generale sulla Protezione dei Dati (di seguito: Regolamento o RGPD),[1] con particolare attenzione alle realtà pubbliche. L'obiettivo è quello di fornire sia ai titolari/responsabili del trattamento, sia agli stessi RPD uno strumento utile per esercitare nel miglior modo possibile il proprio ruolo e le proprie funzioni a supporto della *compliance* dell'ente in cui si opera.

Sui diversi temi affrontati, si è tenuto conto delle indicazioni provenienti dal Garante per la protezione dei dati personali (di seguito: Garante), dal Comitato europeo per la protezione dei dati (di seguito: Comitato europeo)[2] e dal Garante europeo[3]; tuttavia, ciò che qui si intende condividere sono le prime esperienze maturate sul campo dai RPD del Network delle autorità amministrative indipendenti e degli organismi affidatari di funzioni ad esse riconducibili, mettendo a disposizione i frutti di un percorso di confronto, approfondimento e definizione di *best practice* che ha caratterizzato sempre l'attività del Network.[4]

Naturalmente, ciascun titolare o responsabile[5] potrà individuare, nella sua autonomia e in relazione alla sua realtà organizzativa, lo strumento (procedura/regolamento interno, prassi, etc.) più adeguato a definire le regole che presiedono allo svolgimento dei compiti del RPD ed alle interrelazioni con le diverse funzioni ad esso attribuite (operative, di staff, etc.).

1. Obbligatorietà della nomina del RPD nella PA

La figura del RPD non rappresenta una novità nelle istituzioni europee: si tratta di un elemento fondamentale nel quadro della protezione dei dati personali presente, sia pure con alcune differenze rispetto al disegno attuale, da oltre 15 anni. Il RGPD lo ha reso un elemento portante della *governance* del "sistema privacy" in tutte le realtà pubbliche e nella maggior parte di quelle private e costituisce, nel nostro Paese, sicuramente una delle misure di più elevato impatto della nuova normativa, che ne prevede l'operatività in stretta connessione con il titolare o il responsabile del trattamento. Comprendere tale legame è una delle sfide del RGPD.

Le *Linee-guida sui responsabili della protezione dei dati*, adottate dal Comitato europeo[6], delineano le caratteristiche peculiari di tale figura come una sorta di **consulente e, al contempo, di un supervisore indipendente, un vero e proprio presidio di legalità, pur nella sua indipendenza ed imparzialit**à che si pone, nell'ambito di ciascuna realtà organizzativa, come punto di riferimento per il titolare, ma anche per gli interessati e per il Garante.

Va sottolineato come il settore pubblico assume la veste di destinatario privilegiato dell'obbligo della sua istituzione: infatti l'art. 37, paragrafo 1, del Regolamento prescrive che *"il titolare del trattamento*

[1] Artt. 37 – 39 e Cons. 97 del Regolamento
[2] European Data Protection Board o EDPB.
[3] European Data Protection Supervisor o EDPS.
[4] Il Network dei RPD delle Autorità indipendenti, istituito a Roma il 15 giugno 2018, su libera iniziativa di alcuni RPD, registra ad oggi l'adesione delle principali autorità di settore e di alcuni organismi che ne supportano l'attività.
[5] Ovviamente le valutazioni e le indicazioni riferite al titolare possono essere applicate anche ai responsabili del trattamento dati in relazione agli obblighi loro assegnati dal Regolamento.
[6] Adottate il 13 dicembre 2016 ed emendate il 5 aprile 2017 ("**WP243rev.01**") dalle autorità nazionali di controllo degli Stati membri dell'Unione europea riuniti nell'allora Gruppo di lavoro articolo 29 (*Working Party*), queste Linee-guida sono state fatte proprie dal Comitato europeo per la protezione dei dati, che dal 25 maggio 2018 ha sostituito il predetto *Working Party*.

e il responsabile del trattamento designano sistematicamente un RPD ogniqualvolta … il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico"[7].

Per i soggetti privati l'obbligatorietà della designazione è strettamente correlata ad alcune tipologie di trattamenti, ad esempio quando il titolare effettua, nel contesto delle proprie *attività principali*, trattamenti che comportano *"il monitoraggio regolare e sistematico degli interessati su larga scala"*, oppure trattamenti *"su larga scala, di categorie particolari di dati personali di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'art. 10"* del Regolamento.

Occorre comunque sottolineare come, anche in assenza di uno specifico vincolo normativo, la designazione di un RPD venga incoraggiata quale concreta espressione del principio di responsabilizzazione (c.d. accountability) a cura del titolare. Infatti, il Comitato europeo, nelle sue Linee Guida, sottolinea come il RPD rappresenti una figura in grado *di "facilitare l'osservanza della normativa e aumentare il margine competitivo delle imprese"* e raccomanda, in termini di buone prassi, che gli organismi privati incaricati di pubbliche funzioni o che esercitano pubblici poteri nominino sempre un RPD.[8]

La rilevanza del ruolo emerge dallo stesso Regolamento laddove la sua designazione è qualificata quale obbligo del titolare/responsabile la cui violazione ricade nell'ambito di applicazione dell'art. 83, par. 4 lett. a), del RGPD e soggetta, pertanto, all'applicazione della sanzione amministrativa pecuniaria fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo (se superiore).

L'obbligo normativo non si limita alla sua formale designazione, ma punta anche alla sua effettività: il titolare/responsabile è tenuto a coinvolgere il RPD *"tempestivamente e adeguatamente" "in tutte le questioni riguardanti la tutela dei dati personali"*[9]. Ciò proprio al fine di assicurare la sostanziale protezione dei dati personali oggetto di trattamento e, al contempo, offrire garanzie che le attività di *compliance* svolte all'interno della struttura organizzativa, dall'attribuzione dei ruoli e delle responsabilità, ai piani di sensibilizzazione e formazione, alle attività di controllo, etc., siano oggetto di una *independent review* da parte del RPD. Ossia proprio di quella figura che, nell'ambito dell'organizzazione, è chiamato a offrire un costante supporto al fine di applicare correttamente la disciplina di riferimento.

Non a caso, il RPD costituisce il *punto di contatto* per l'autorità nazionale di controllo (il Garante) *per questioni connesse al trattamento* dei dati personali, come prevede l'art.39, paragrafo 1, lettera e), del RGPD.

Ne deriva, pertanto, che il coinvolgimento del RPD, ogniqualvolta si trattino dati personali, debba costituire una priorità da parte del titolare e risponda ad un suo esclusivo interesse.

Tale quadro interpretativo trova conferma in un provvedimento del Garante del 2020: l'aver coinvolto il RPD nell'ambito delle attività di trattamento di dati personali è stato considerato quale elemento atto ad attestare la *compliance* al RGPD e tale da comportare una riduzione della sanzione amministrativa pecuniaria comminata al titolare.[10]

Recentemente il Garante,[11] nella progressiva definizione degli obblighi stabiliti dal RGPD, ha censurato il mancato coinvolgimento del RPD in merito alle operazioni di trattamento, quale elemento

---

[7] Unica eccezione le *"autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali*." (lett. a), par. 1, cit.). Eccezione peraltro superata dal D. Lgs. n. 196 del 30 giugno 2003 novellato dal D. Lgs. n. 101 del 10 agosto 2018 (di seguito: "**Codice Privacy**"), che estende l'obbligo di designazione a tali autorità (cfr. art. 2-sexiesdecies).
[8] WP243rev.01, p. 8.
[9] Art. 38, par. 1 e Cons. 98 del Regolamento.
[10] Provvedimento Garante n. 118 del 2 luglio 2020 (Comune di Greve in Chianti).
[11] Provvedimento Garante n. 87 del 25 febbraio 2021 (INPS).

integrante la violazione del principio di *accountability* (inosservanza alla quale si applica la sanzione più elevata di cui all'art. 83, par. 5, RGPD).

2. Competenze del RPD

Il RPD è una figura di garanzia deputata a stimolare (con attività di informazione e consulenza) ed a verificare (mediante attività di sorveglianza) il corretto adempimento della normativa in materia di protezione dei dati personali.

Il Regolamento non prevede specifici requisiti o attestazioni/certificazioni per il RPD ma dedica ampi spazi a delinearne il profilo e le caratteristiche professionali.

Innanzitutto, tale soggetto deve, proprio per poter garantire il corretto e pieno svolgimento dei compiti a lui affidati dall'art. 39, **possedere un'approfondita conoscenza della normativa e delle prassi in materia di protezione dei dati, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento**.

Ma tale competenza, pur fondamentale, non è di per sé sufficiente: il ruolo che gli assegna il RGPD richiede un grado di professionalità poliedrico e, dunque, adeguato alla complessità del compito da svolgere e la capacità di fornire al titolare (o al responsabile) quella consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvandolo nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Contemporaneamente il RPD deve *cooperare* con il Garante e fungere da interfaccia fra i soggetti, interni ed esterni all'organizzazione, i cui dati sono oggetto di trattamento: non si dimentichi che oltre alle autorità di controllo, infatti, anche i soggetti interessati possono rivolgersi direttamente al RPD. [12]

Il RPD deve anche avere l'**autorevolezza** per agire in piena indipendenza (art. 38, par. 3 e Cons. 97 del Regolamento) e autonomia, non potendo ricevere istruzioni e riferendo direttamente ai vertici dell'ente: a tal fine deve possedere oltre alle qualità professionali e alla conoscenza della struttura (compresi gli aspetti IT e le misure di sicurezza), anche capacità organizzative e di comunicazione.[13]

La conoscenza, anzi l'essere parte della realtà organizzativa, costituisce sicuramente un elemento (in particolare per la PA) che può favorire e porta a privilegiare la sua scelta all'interno della struttura. Tuttavia, se le competenze e le qualità necessarie non fossero disponibili nell'organigramma interno, potrebbe essere consigliabile una individuazione esterna.[14]

Il titolare deve *sostenere* il RPD e si deve assicurare che abbia a disposizione le **risorse necessarie per assolvere ai suoi compiti**. Tra le risorse devono essere comprese le risorse finanziarie per una sua formazione continua, da garantire fin dall'avvio dell'attività, da aggiornare costantemente e accrescere nel tempo; tali impegni di spesa devono confluire nel generale Piano di formazione e

---

[12] Art. 39 RGPD e WP243rev.01, *Introduzione*.

[13] FAQ n. 2 del Garante relativa ai RPD in ambito pubblico: *"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."* (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110#b).

[14] Art. 37, par. 6 del Regolamento "*può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizio*".
Il Garante europeo, nel *Position Paper on the role of Data Protection Officers of the EU institutions and bodies*, 18 settembre 2018 ("**EDPS Position Paper**"), afferma espressamente che al fine di assicurare un'adeguata conoscenza del funzionamento dell'ente, il RPD dovrebbe essere, nella misura più ampia possibile, una risorsa interna di staff e l'esternalizzazione della funzione dovrebbe essere limitata allo stretto necessario (p. 7). Questo documento, sia pure rivolto principalmente ai RPD degli organismi europei, contiene spunti utili anche per i RPD degli Stati membri, essendo le norme in gran parte coincidenti.

aggiornamento del personale e trovare apposita copertura nel bilancio. Auspicabile sarebbe l'istituzione di un capitolo dedicato con risorse per formazione e supporto in termini di personale e strumenti di gestione.

Da tale quadro, che pone in evidenza una multidisciplinarietà di competenze che devono caratterizzare tale figura, emerge, nell'interesse stesso del titolare e a dimostrazione della sua *accountability*, la necessità di supportare il RPD con un *gruppo di staff* o una segreteria tecnica (anche non esclusiva, ma comunque presente ogniqualvolta necessario) che veda la presenza qualificata delle diverse professionalità di volta in volta richieste. La composizione è da valutare in relazione anche alle caratteristiche dell'organizzazione: sicuramente non può mancare la presenza di un legale, di un informatico e/o di un esperto di sicurezza.

Occorre comunque sottolineare il ruolo fondamentale che deve svolgere, nella struttura organizzativa del titolare, il *senior management* al fine di garantire il massimo supporto e collaborazione al RPD nello svolgimento della propria attività. È opportuno che il titolare, nella definizione del suo Sistema Privacy, si assicuri anche di riportare tali indicazioni nell'ambito delle istruzioni fornite alle persone fisiche da lui autorizzate ovvero designate[15], *sotto la sua autorità e nell'ambito del proprio assetto organizzativo,* a trattare dati personali.

In prospettiva, potrebbe rivelarsi utile individuare un *referente privacy* interno, adeguatamente formato, col compito di coadiuvare la propria Area o Dipartimento nelle attività di *compliance* al RGPD e di assicurare che la struttura presti la dovuta attenzione agli *input* del RPD.

Nulla dice il Regolamento sulla durata dell'incarico di RPD. Ogni valutazione è rimessa, come sempre, al prudente apprezzamento del titolare, che dovrà tenere conto della forte caratterizzazione di indipendenza e terzietà di tale figura, non tralasciando di valutare quanto già investito in termini di formazione e conoscenza. A tale riguardo, il Garante europeo raccomanda di nominare il RPD per una durata più ampia possibile.[16]

3. Posizionamento del RPD nell'ambito dell'organizzazione e conflitti di interesse

La possibilità di svolgere in modo adeguato i propri compiti dipende in misura rilevante dall'autonomia e dal posizionamento del RPD all'interno della struttura organizzativa nonché dalla possibilità di una efficace correlazione con le altre funzioni, incluse quelle di 2° e 3° livello (ad esempio: Controllo di gestione, Gestione rischi operativi, Responsabile della Prevenzione della Corruzione e Trasparenza).

3.1. Autonomia e indipendenza

Come prevede l'art. 38, paragrafo 3 del RGPD, il RPD deve essere collocato in una posizione che lo ponga nelle condizioni di svolgere le sue funzioni: ***a)*** **senza ricevere istruzioni** né subire impulsi o condizionamenti di ogni tipo dalle altre Strutture o da altri soggetti sull'interpretazione da dare a una specifica questione alla luce della normativa in materia di protezione dei dati o sull'approccio da seguire nel caso specifico; ***b)*** **riferendo direttamente al vertice** gerarchico del titolare (o del responsabile).

[15] A completamento dell'art. 29 RGPD, secondo cui titolare e responsabile devono istruire coloro che (sotto la loro autorità), accedono ai dati personali, il **Codice Privacy** stabilisce all'art. 2-*quaterdecies* che titolare e responsabile possono prevedere, nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche espressamente designate.
[16] EDPS Position Paper, p. 1.

La posizione di indipendenza nella struttura non riguarda soltanto il divieto di ricevere istruzioni da parte di un superiore, ma implica anche che il RPD non debba essere in una posizione tale da essere influenzabile nel momento in cui si rapporta al *management.*[17] A garanzia del RPD, il divieto di rimozione o penalizzazione in rapporto all'adempimento dei propri compiti previsto nell'art. 38 paragrafo 3, va inteso in senso ampio: si pensi ad una mancata o ritardata promozione, ad un blocco delle progressioni di carriera, ad una mancata concessione di incentivi rispetto ad altri dipendenti.[18]

Tali tutele sono essenziali per consentire al RPD di manifestare il proprio dissenso qualora il titolare. o le persone da lui designate ad operare, assumano decisioni difformi dalle indicazioni fornite[19] e di evidenziarne posizioni in contrasto con il RGPD, garantendo di poter interloquire direttamente con il vertice amministrativo (ad esempio, il consiglio di amministrazione per le aziende e il collegio per le autorità amministrative indipendenti) e di rendicontare nella sua Relazione annuale sulle attività svolte e sul grado di *compliance* della struttura, da sottoporre al vertice gerarchico almeno una volta all'anno.

La circostanza che il Regolamento espressamente stabilisca che il RPD sia tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, caratterizza e rafforza ulteriormente la sua figura all'interno dell'Organizzazione.

3.2. Competenze del RPD

L'art. 38, paragrafo 6 del RGPD consente che il titolare possa affidare al RPD altri compiti e funzioni all'interno dell'organizzazione. Tuttavia, risulta indispensabile che il titolare si assicuri, in primo luogo, che tali compiti e funzioni non presentino tra loro conflitti di interesse.

A tal fine, importanza cruciale riveste il principio in base al quale il RPD non può ricoprire ruoli che, all'interno dell'ente, gli consentano di determinare le finalità ed i mezzi del trattamento di dati personali o, comunque, di incidere direttamente su tali aspetti: ciò in quanto egli eserciterebbe poteri decisionali sui quali potrebbe contestualmente essere chiamato a vigilare in ordine alla loro aderenza al quadro normativo vigente. In altri termini, il RPD si troverebbe nella singolare, e non accettabile situazione, di fungere sia da "controllore", sia da "controllato". Si tratta, invece, di figure che devono essere tenute ben distinte, proprio per non svilire il senso del RPD.

Su tali basi, risulta di difficile compatibilità con la funzione di RPD sia la contemporanea titolarità di ruoli quali, ad esempio, amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT[20] o, con particolare riferimento alle Autorità amministrative indipendenti, rivestire il ruolo di Presidente o altro membro del Collegio, Segretario generale, Direttore generale, sia anche l'essere titolare di posizioni gerarchicamente inferiori nel caso in cui abbiano il potere di determinare finalità o mezzi del trattamento.

Di contro, al RPD ben possono essere assegnate anche posizioni apicali purché non "assorbenti" e non venga ad esso attribuito il potere di determinare finalità o mezzi del trattamento.

In linea generale, anche al fine di agevolare le valutazioni sul punto, si ritiene buona prassi per i titolari identificare, in via preventiva e strutturale nei vari regolamenti di organizzazione, le posizioni ritenute incompatibili con la funzione di RPD.

Anche il Garante europeo si è occupato espressamente di delineare i casi di possibile conflitto di interesse nell'attività del RPD laddove, ad esempio, ha previsto che quest'ultimo non possa

[17] EDPS Position Paper, p. 9.
[18] WP243rev.01, p. 20.
[19] WP243rev.01, p. 17.
[20] Cfr. WP243rev.01, p. 22.

rappresentare l'organismo nell'ambito di un procedimento giudiziario riguardante un contenzioso in materia di protezione dei dati. Infatti, tale compito risulta difficilmente conciliabile con l'indipendenza del RPD, anche nel caso in cui questi non sia stato previamente coinvolto nella questione. Rappresentare in giudizio ed agire per conto dell'istituzione in casi correlati alla protezione dei dati comprometterebbe comunque l'indipendenza e l'imparzialità del RPD. In altri termini, il RPD non tutela direttamente gli interessi del titolare in cui è incardinato, ma tutela i dati personali e la *compliance* al relativo sistema normativo da parte dell'ente che lo ha designato. Ciò si traduce anche in una tutela indiretta del titolare, che viene avvertito dal RPD delle lacune nella *compliance* e, quindi, messo in condizioni di rettificare scelte non coerenti con la disciplina vigente.

Sotto un analogo profilo, va adeguatamente assicurato che il RPD sia effettivamente in grado di svolgere le proprie funzioni e, quindi, che le ulteriori funzioni attribuitegli non inibiscano tale possibilità, come previsto dall'art. 38 del RGPD. Gli eventuali compiti ulteriori assegnati al RPD non possono, quindi, né impedire né intralciare l'attività propria; è pertanto utile che, laddove rivesta anche ulteriori ruoli, il RPD pianifichi la propria attività, definisca una percentuale massima di tempo lavorativo dedicato all'esercizio del suo ruolo[21]e disponga correlativante di risorse aggiuntive adeguate.

Alla luce delle due condizioni poste dal Regolamento (divieto di conflitto di interessi e necessità di avere a disposizione tempo sufficiente per l'espletamento dei propri compiti) risulta difficile, negli enti di grandi dimensioni, assegnare al RPD ulteriori responsabilità, che potrebbero generare un cumulo di impegni tale da incidere negativamente sull'effettività dello svolgimento dei suoi compiti.[22]

Infine si sottolinea come, nell'organigramma del Garante,[23] il RPD viene collocato in una posizione che ne evidenzia il diretto rapporto con l'Organo di vertice (il Collegio), in chiave di supporto e di consulenza rispetto a quest'ultimo. Si rende in tal modo, anche graficamente, evidenza chiara dei connotati di autonomia e indipendenza rivestiti necessariamente dal RPD.

3.3. Rapporti con altri ruoli interni

Proprio con l'obiettivo di assicurare il più efficace esercizio delle sue funzioni, con particolare riferimento a quelle di sorveglianza sulla corretta applicazione del RGPD, è necessario che il RPD sia posto nelle condizioni di rapportarsi in modo veloce ed efficace con le strutture interne che trattano dati personali, ma soprattutto quelle che, sotto diverse aspetti e sulla base di normative specifiche, svolgono attività correlate a quelle del RPD, quali ad esempio la funzione interna di *audit* o gli eventuali *auditor* esterni. Con tali soggetti il RPD, al pari del titolare, dovrebbe avere un rapporto diretto.

Si ritiene buona prassi prevedere flussi informativi costanti fra il RPD e tali strutture, nel rispetto dei ruoli e delle attribuzioni, volti alla condivisione delle informazioni rilevanti ed all'analisi comune e integrata di temi e criticità, in vista di una loro risoluzione in via sinergica.

In particolare, un coinvolgimento limitato ma mirato del RPD in alcune fasi del processo di *audit* che concernono i profili di *compliance* con la normativa in materia di trattamento dei dati personali, potrebbe contribuire a dare più vigore e concretezza a quella attività di sorveglianza sull'osservanza

[21] WP243rev.01, p. 14.
[22] Tale cumulo potrebbe aversi, ad esempio, avuto riguardo, caso per caso, alla specifica struttura organizzativa, alla dimensione e alle attività del singolo titolare o responsabile, come nel caso in cui si attribuisca al medesimo soggetto le funzioni di RPD e di Responsabile per la Prevenzione della Corruzione e per la Trasparenza, considerata la molteplicità degli adempimenti che incombono su tale figura. Vedi Garante, FAQ sul Responsabile della Protezione dei dati (RPD) in ambito pubblico, in particolare FAQ n. 7.
[23] https://www.garanteprivacy.it/documents/10160/0/Organigramma+aggiornato+al+3+febbraio+2021.pdf/9b73c646-0118-1049-d631-b4df899ab4fd?version=1.0.

della medesima normativa, alla quale il RPD è chiamato ai sensi dell'art. 39, par. 1, lett. b) del RGPD, a tutto vantaggio dell'efficacia e della non invasività dei controlli. La trasmissione della Relazione annuale del RPD anche alla funzione di *audit* può costituire uno strumento efficace di circolazione delle informazioni.

4. Compiti e funzioni del RPD

Il RPD assiste il titolare nell'attività di *compliance* alla normativa in tema sulla protezione dei dati personali.

I suoi compiti sono elencati all'articolo 39, paragrafo 1 del Regolamento, ma l'elenco non è esaustivo e nulla vieta che – lo si ribadisce – gli siano assegnate funzioni ulteriori, purché tali da non dare adito a conflitti di interesse[24] e in grado di consentire al RPD di disporre del tempo sufficiente all'espletamento dei compiti a lui affidati dal Regolamento.[25]

Sia che gli siano attribuiti solo i compiti "tipici", sia che se ne estenda l'ambito di operatività, attribuzioni e compiti assegnati al RPD devono essere portati con chiarezza a conoscenza del personale dell'organizzazione (es. fornendo informative ai dipendenti).[26]

4.1. Compiti tipici (obbligatori)

Per consentire al RPD di assolvere ai suoi compiti, è necessario (come già sottolineato) che tutti i soggetti designati/autorizzati ad assumere decisioni in ordine alle finalità ed ai mezzi del trattamento (nell'ambito del titolare) o a trattare i dati personali (nell'ambito del responsabile) informino e coinvolgano tempestivamente il RPD in tutte le questioni che riguardano la protezione dei dati personali.[27]

Premessa questa indispensabile per mettere in condizione il RPD di svolgere quei **compiti informativi e consulenziali**, previsti dall'art. 39, paragrafo 1, lett. a) a beneficio del titolare (o del responsabile) e dei dipendenti che eseguono il trattamento. Il RPD ha dunque in primo luogo il ruolo di contribuire a sviluppare, nella realtà in cui opera, la cultura della protezione dei dati.

Diverse le modalità con cui operare: redazione di note informative periodiche o ad hoc, sessioni formative, pagine dedicate sulla intranet,[28] come anche offrire un'attività generalizzata di consulenza e di supporto rivolta a tutto il personale.

Il Regolamento e le Linee guida europee prevedono casi di consultazione necessaria o, comunque, fortemente raccomandata del RPD: l'obbligo è espressamente previsto nel caso dello svolgimento di una valutazione di impatto sulla protezione dei dati personali (di seguito: DPIA)[29] e sussiste certamente al verificarsi di un possibile *data breach.*[30]

Il RPD deve assistere il titolare nello svolgimento della DPIA, in particolare nelle scelte più rilevanti: se ricorrono o meno le condizioni per effettuarla, la metodologia da adottare, se condurla con risorse interne o esterne, quali garanzie applicare (incluso le misure tecniche e organizzative) per attenuare i rischi per gli interessati; successivamente soccorre nella valutazione della sua corretta conduzione e delle conclusioni raggiunte. Nell'ipotesi in cui il titolare del trattamento non concordi con le

[24] Art. 38, par. 6.
[25] Art. 38, par. 2.
[26] WP243rev.01, p. 23.
[27] Tale obbligo è espressamente previsto per titolari e responsabili dall'art. 38 del Regolamento.
[28] EDPS Position Paper, p. 13.
[29] *Data Protection Impact Assessment* (art. 39, par. 1, lett. c) e art. 35, par. 2).
[30] WP243rev.01, p. 18: *"occorrerà garantire, per esempio [omissis] che il RPD sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente."*

indicazioni fornite dal RPD, la documentazione relativa alla DPIA dovrà riportare le motivazioni per cui il titolare ha ritenuto di non conformarsi a tali indicazioni. Peraltro, il parere del RPD dovrebbe ricevere *sempr*e la dovuta considerazione e, in caso di disaccordo, il titolare, quale buona prassi, dovrebbe documentare le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal RPD.[31]

A livello nazionale, un ulteriore obbligo di consultazione del RPD è fissato nelle Linee Guida sui documenti informatici adottate dall'Agenzia per l'Italia Digitale (AgID) nel 2020.[32] Tali Linee-guida prevedono che il Responsabile della gestione documentale e il Responsabile della conservazione debbano acquisire il parere del RPD ai fini di predisporre il Manuale di gestione documentale ed il Piano della sicurezza del sistema di gestione informatica dei documenti.[33]

Merita attenzione il compito del RPD di **sorvegliare l'osservanza del Regolamento** (art. 39, paragrafo 1, lett. b)). Si tratta di un compito di controllo e monitoraggio che può essere svolto in diverse modalità: raccolta di informazioni sui trattamenti posti in essere anche tramite l'accesso al Registro dei trattamenti; analisi e verifica di conformità rispetto alla normativa sulla protezione dei dati personali; sorveglianza sull'attività di risposta alle richieste degli interessati; verifica della *governance* interna; verifica delle procedure di *compliance* alla normativa sulla protezione dei dati personali da parte del titolare. In questa attività quale utile parametro di valutazione, oltre alle norme, alle linee guida in materia e alle procedure del titolare[34] è opportuno far riferimento alla prassi interpretativa degli organismi e delle autorità nazionali e comunitarie di settore.

Occorre sottolineare come il controllo del rispetto del Regolamento non significa che il RPD sia personalmente responsabile in caso di inosservanza: il rispetto delle norme in materia di protezione dei dati resta infatti in capo al titolare del trattamento (art. 24, paragrafo 1). Sicuramente il RPD ha il compito di segnalare al titolare inadempienze, difformità e scostamenti dal RGPD e dalle buone prassi. Necessario che il RPD tenga traccia di tali segnalazioni o indicazioni, proprio al fine di testimoniare il coinvolgimento del RPD da parte del titolare, anche se nulla espressamente prevede la normativa al riguardo.

Riveste rilievo, come già sottolineato, la funzione di raccordo tra titolare e Garante svolta dal RPD. 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".*

Ma non soltanto: il RPD, proprio per la sua professionalità, esperienza e conoscenza della materia della tutela dei dati personali e delle attribuzioni dell'organizzazione in cui opera, sarà in grado di fornire ogni opportuno chiarimento al Garante e indirizzare l'attività nella modalità più adeguata ad assicurare la *compliance* al regolamento.

Questi compiti attengono al ruolo di "*facilitatore"* attribuito al RPD, ma sarà sempre il titolare, anche se affiancato dal RPD, a rapportarsi con il Garante e a individuare la persona che, nella propria

---

[31] *Ibidem.*

[32] Linee guida sulla formazione, gestione e conservazione dei documenti informatici pubblicate l'11 settembre 2020. L'attuazione di queste Linee-Guida entro il prossimo 7 giugno 2021 è obbligatoria – tra gli altri – per le pubbliche amministrazioni (incluso le autorità amministrative indipendenti), i gestori di servizi pubblici, le società a controllo pubblico e, secondo il Consiglio di Stato, dovrebbero essere vincolanti *erga omnes* (parere del Consiglio di Stato n. 2122/2017 del 10/10/2017, punto 5.1).

[33] Paragrafi 3.4, 3.9 e 4.10 alle pagine 25-26, 30 e 39 delle Linee-guida. Come noto, i documenti citati (Manuale di gestione documentale e Piano della sicurezza del sistema di gestione informatica dei documenti) si coordinano con il Piano di conservazione (che per le PA è allegato al Manuale di gestione documentale – v. Linee-Guida Agid, p. 28) e completano il disegno di gestione e conservazione in sicurezza del patrimonio informativo pubblico.

[34] Nello svolgimento di questa funzione, il RPD può preparare delle checklist o delle FAQ tematiche per guidare il titolare nella verifica del corretto adempimento.

organizzazione, sia in grado di produrre al Garante le informazioni richieste, soprattutto nell'ambito di ispezioni, gestione dei reclami, DPIA e consultazione preventiva.

4.2. Compiti ulteriori (facoltativi)

Oltre ai compiti previsti dal Regolamento o individuati dalla legge nazionale, il titolare può chiedere al RPD di svolgere ulteriori compiti attinenti al suo ruolo.

Tra i più diffusi, quello di curare la tenuta ed aggiornamento del **Registro dei trattamenti,** sulla base delle informazioni fornite dai vari uffici che trattano dati personali. Soprattutto in strutture complesse (organizzate in aree, dipartimenti, direzioni, etc.), in cui il titolare, ai sensi dell'art. *2 quaterdecies* del Codice Privacy abbia designato i dirigenti ad occuparsi, ciascuno per la parte di competenza, anche dell'elaborazione del Registro dei trattamenti, il RPD potrebbe operare come collettore delle informazioni ed organizzatore del Registro (unitario) dell'organizzazione. Tale scelta è coerente con le funzioni tipiche del RPD, in quanto il Registro è uno degli strumenti che gli consentono di adempiere agli obblighi di sorveglianza del rispetto del Regolamento.

È importante, tuttavia, sottolineare che, anche laddove il RPD sia incaricato di supportare la tenuta e l'aggiornamento del Registro, **tali attività restano di esclusiva responsabilità del titolare**: il RPD potrà fungere da stimolo (es. invitare periodicamente all'aggiornamento le funzioni competenti) e da raccordo delle informazioni (anche a fini di omogeneità dei contenuti tra funzioni diverse), ma non sarà responsabile dei contenuti. Nei casi in cui il Registro sia invece tenuto da altra funzione, ben potrà il RPD accedervi e fornire i propri suggerimenti, nell'esercizio dei suoi compiti di indirizzo e consulenza nei confronti del titolare.

Un secondo ambito di possibile estensione delle attività del RPD riguarda i **diritti degli interessati**. I dati di contatto del RPD sono ricompresi tra i contenuti obbligatori delle informative che devono essere rese agli interessati (interni ed esterni all'organismo), i quali possono contattarlo in relazione ad ogni aspetto inerente al trattamento dei loro dati personali ed all'esercizio dei propri diritti.[35] La circostanza che il RPD agisce all'interno dell'organizzazione lo colloca in una posizione ideale sia per ricevere e gestire richieste e reclami, sia per tracciarne casistiche ed esito con la redazione di un apposito Registro.

Occorre comunque ribadire anche su questo tema che il RPD non può mai sostituirsi al titolare nell'adempimento dei suoi obblighi: può agire da "interfaccia" rispetto agli interessati ma non può avere la responsabilità di rispondere alle loro richieste. In questi casi, l'RPD dovrà coordinarsi con la funzione interna competente, attivandola e (se occorre) sollecitandone l'azione.

Sicuramente, inoltre, il RPD può svolgere un'attività di coordinamento delle risposte da parte degli uffici competenti, anche a fini di omogeneità contenutistica e formale. Tale attività va tenuta distinta dalle risposte alle richieste di consulenza interne, cui l'RPD dovrà rispondere con l'autonomia ed indipendenza proprie del suo ruolo.

Non estraneo al ruolo, anzi in linea con il suo compito di sensibilizzazione, il coinvolgimento diretto del RPD nella redazione e nell'organizzazione del Piano formativo dell'organizzazione. Può, se del caso, essere lui stesso a pianificare la docenza e curare direttamente la formazione di tutto il personale e/o dei *referenti privacy* (ove nominati), oppure coordinarsi con la funzione competente (di regola le risorse umane) per la selezione dei docenti, dei contenuti e delle modalità di fruizione degli eventi formativi.

[35] Tale facoltà di contattare il RPD è prevista espressamente dall'art. 38 par. 4. Il Garante europeo raccomanda come buona pratica di fornire un canale sicuro di comunicazione col RPD, come ad esempio un indirizzo e-mail o un sistema interno dedicato di comunicazioni/chat (EDPS Position Paper, p. 13).

5. Modalità di coinvolgimento del RPD e sua *accountability*

Il RPD può esercitare il suo ruolo solo nel caso in cui, come già più volte evidenziato, viene messo a conoscenza di ogni questione attinente al trattamento di dati delle persone fisiche e se dispone tempestivamente di tutte le informazioni pertinenti: è la premessa indispensabile per poter operare correttamente le proprie valutazioni e rendere una consulenza adeguata.

Occorre, quindi, che il RPD non sia solo informato ma venga coinvolto sia nei casi di modifica dei trattamenti in atto, sia laddove gli uffici siano chiamati a svolgere attività non specificamente indicate nel Registro dei trattamenti (e dunque, non ancora valutate quanto a presidi di garanzia) qualora dette attività richiedano anche solo la mera acquisizione incidentale di dati personali, pur non essendo gli stessi oggetto dell'attività svolta dall'ente o strettamente attinenti ad essa. Il trattamento rilevante, ai sensi del RGPD, non necessita, infatti, che i dati siano oggetto di istruttoria o di una qualche altra forma di considerazione: nel momento in cui pervengano nella struttura, deve attivarsi il meccanismo che presiede al loro trattamento, cioè alla loro tutela. Laddove ciò avvenga nell'ambito di un processo non mappato nel Registro dei trattamenti, il vertice dell'ufficio preposto dovrà sollecitamente informarne il RPD e comunicargli i presidi adottati.

Tutti dipendenti dell'Organizzazione devono essere in tal senso sensibilizzati dal titolare.

Potrebbe rivelarsi utile definire procedure interne per le consultazioni formali del RPD su specifici atti (ad esempio casi di consultazione obbligatoria),[36] anche al fine di ottimizzare i relativi tempi e modalità, chiarendo che il parere del RPD su un atto dovrebbe essere richiesto dal responsabile dell'atto o dal suo delegato.

Particolare rilievo assumono a riguardo le Linee guida del Comitato europeo laddove, proprio al fine di garantire e ribadire rilevanza e significato del necessario coinvolgimento del RPD, raccomandano che il RPD **sia regolarmente invitato alle riunioni di management di alto e medio livello**.[37]

Analoga posizione è stata assunta dal Garante europeo per il quale il RPD dovrebbe essere visto come "*discussion partner*" all'interno dell'ente e far parte dei gruppi di lavoro, *steering committees*, etc., che si occupano di attività di trattamento. E cita come buona prassi, ad esempio, la consultazione del RPD nella fase di pianificazione di un sistema IT, al fine di avere un aiuto nell'identificare e valutare se siano o meno trattate informazioni personali, le categorie di dati raccolti, la finalità del trattamento, etc.[38] Anche (ma non solo) in questa consultazione, il RPD potrebbe aiutare l'organizzazione ad attuare non solo obblighi specifici, ma anche principi posti dal RGPD, tra cui quelli rientranti nelle nozioni di *privacy by design* e *by default*.

È ovvio che tale coinvolgimento riporta l'attenzione sulla posizione del RPD nella scala gerarchica dell'amministrazione e mal si concilia con posizioni che non siano apicali.

Occorre evidenziare come la figura del RDP si pone a garanzia e stimolo non solo della *compliance* dell'organizzazione agli adempimenti normativi ma, soprattutto, a tutela del titolare nel preservare e far buon uso del proprio patrimonio informativo, stimolando e indirizzando verso comportamenti e soluzioni a tutela non solo di chi opera all'interno della struttura, ma soprattutto di chi fruisce dei servizi da essa offerti. Ciò è essenziale per l'obiettivo di rafforzare il clima di fiducia, indispensabile premessa anche per i rapporti tra PA e cittadini.

---

[36] Così il WP243rev.01, p. 18.
[37] WP243rev.01, p. 18.
[38] EDPS Position Paper, p. 8.

In un clima di reciproca fiducia e trasparenza, assume rilievo ancora una volta il principio di *accountability* che pervade tutto il Regolamento.

Ed è proprio in tale ottica che si ritiene necessario che anche il RPD relazioni e conservi memoria della sua attività e delle posizioni espresse. Rendere conto significa, infatti, dimostrare le proprie attività e, per poterlo fare, occorre tenerne traccia.

Tenere doverosa traccia dell'attività sfocia per l'RPD in due azioni sinergiche:

1) predisporre, almeno annualmente, una Relazione al titolare che dia conto del grado di *compliance* al regolamento dell'intera organizzazione evidenziando criticità e progressi, in particolare sul fronte della *governance* e della formazione, delineando le azioni e le priorità da perseguire e il programma di monitoraggio sull'osservanza della normativa sulla protezione dati per l'anno successivo;
2) conservare i documenti (note, e-mail) che attestino le attività svolte. In base all'autonomia di cui gode, il RPD potrà valutare se organizzare tali documenti in un elenco/repertorio (ad esempio organizzato cronologicamente o per settore di intervento).

A quest'ultimo riguardo, la traccia di ogni singola attività svolta risulta essenziale, ove si consideri che l'intervento del RPD nell'organizzazione può avvenire, da un lato, a fronte di specifiche richieste di consulenza, dall'altro lato, con attività in via autonoma.

Oltre all'indirizzo dedicato (rpd@.....it) o all'e-mail professionale nominativa del RPD potrebbe essere opportuno, in relazione anche alle diverse realtà organizzative, che il RPD disponga di un indirizzo pec (dedicato o meno), al fine di poter riscontrare eventuali richieste provenienti da pec.

Nel caso in cui il RPD si attivi di propria iniziativa, può operare anche periodicamente ricordando ai responsabili delle unità organizzative – con modalità anche informali, ma idonee a lasciare traccia, ad esempio via e-mail – di essere informato su qualunque attività comporti il trattamento di dati personali. Oppure può sollevare quesiti specifici ove le evidenze del caso lo richiedano. Anche i componenti del gruppo di supporto di cui il RPD sia eventualmente dotato o gli stessi *referenti privacy*, ove designati, possono farsi parte attiva nel segnalargli eventuali iniziative adottate nell'ambito degli uffici dell'ente di cui siano venuti in vario modo a conoscenza. Queste attività non codificate, ma essenziali per sostanziare il ruolo del RPD, non solo devono essere rese in forma scritta, come detto, ma la relativa documentazione dovrebbe essere conservata – anche nella sola modalità informatica – e, se del caso, puntualmente riportata nell'elenco/repertorio delle attività svolte dal RPD.

La descrizione dell'attività (e dell'impegno) del RPD nel contribuire a tradurre in realtà l'effettiva conformità al Regolamento dell'ente presso cui opera, trova la sua sede naturale nella Relazione che il RPD stesso dovrebbe rendere annualmente all'organo di vertice. Quale strumento di analisi e verifica periodica, tale relazione deve essere intesa come uno dei più rilevanti contributi all'*accountability* del titolare, uno dei principi fondanti del nuovo Sistema Privacy.