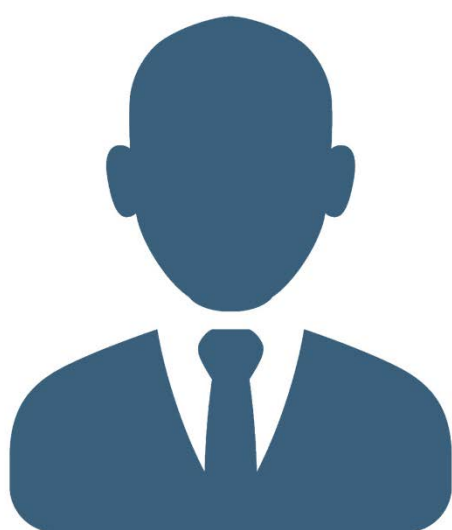




| **GPDP** |

**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**



Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico

Documento allegato al provvedimento del 29 aprile 2021 n. 186

Sommario:

1. Introduzione
2. Una considerazione preliminare: il RPD quale “punto di contatto” per l’Autorità
3. Obbligo di designazione
 - 3.1. Designazione di RPD interno nelle more della conclusione del procedimento di affidamento dell’incarico a RPD esterno
4. Designazione di un unico RPD per conto di più soggetti pubblici
 - 4.1. Comunicazione dei dati di contatto da parte di ciascun titolare in presenza di un RPD selezionato da più titolari
5. Qualità professionali e possesso di titoli
6. Questioni attinenti alla designazione di un RPD esterno
 - 6.1. Allineamento tra contratto di servizi, atto di designazione e pubblicazione/comunicazione al Garante
 - 6.2. Pluralità di enti pubblici per conto dei quali viene svolto l’incarico e pluralità di servizi forniti anche al medesimo titolare
 - 6.3. Individuazione, all’interno del RPD persona giuridica, del referente persona fisica
 - 6.4. Durata dell’incarico
 - 6.5. Remunerazione
7. Pubblicazione e comunicazione all’Autorità dei dati di contatto del RPD
8. Coinvolgimento da parte del titolare e svolgimento dei compiti da parte del RPD
9. Risorse messe a disposizione dal titolare e costituzione di un *team* di collaboratori del RPD
10. Incompatibilità con altri incarichi e conflitto di interessi
 - 10.1. RPD interno che ricopre incarichi per i quali partecipa all’adozione delle decisioni in materia di finalità e modalità del trattamento, o altre decisioni che impattano su trattamenti di dati personali
 - 10.2. RPD esterno che fornisce servizi IT quale responsabile del trattamento
 - 10.3. RPD esterno che rappresenta in giudizio il titolare
 - 10.4. Inquadramento in caso di RPD interno

1. Introduzione

Sin da prima che il Regolamento (UE) 2016/679 iniziasse a dispiegare i suoi effetti (25 maggio 2018), l'Autorità ha dedicato grande attenzione al tema del Responsabile della protezione dei dati (RPD) in ambito pubblico, ritenuto uno snodo fondamentale per l'acquisizione di un corretto approccio al trattamento dei dati personali, soprattutto all'interno di un panorama che vede le pubbliche amministrazioni sempre più sollecitate dalla sfida della c.d. "trasformazione digitale".

Come noto, sul tema, il Regolamento dedica gli artt. 37-39 (oltreché il cons. 97). In proposito, il Gruppo di Lavoro Articolo 29 (WP29) (poi divenuto Comitato europeo per la protezione dei dati) ha emanato le *"Linee guida sui responsabili della protezione dei dati"* (adottate il 13 dicembre 2016 ed emendate il 5 aprile 2017).

Per fare fronte alle prime richieste di chiarimenti giunte nel settore pubblico, al fine di accompagnare il processo di progressivo adeguamento al nuovo quadro regolamentare europeo, il Garante ha successivamente adottato, il 15 dicembre 2017, le *"Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico"* (reperibili su www.garanteprivacy.it, doc. web n. 7322110).

Al contempo, l'Autorità ha promosso numerosi incontri di carattere divulgativo, che hanno riguardato specificamente la figura del RPD, al fine di raggiungere il maggior numero possibile di rappresentanti di enti pubblici. Inoltre, dal punto di vista più strettamente formativo, l'Autorità si è fatta parte attiva all'interno del progetto europeo T4DATA, culminato con la redazione di un Manuale operativo sul RPD (doc. web n. 9152344), la realizzazione di *webinar* formativi e lo svolgimento di eventi di carattere, locale, nazionale e transnazionale.

Ciò premesso, dal 2018 ad oggi, pur a fronte di una maggiore sensibilità al tema, si registrano ancora, nella realtà delle pubbliche amministrazioni, diverse incertezze che impediscono una compiuta realizzazione di questa importante figura e che rischiano di pregiudicare una piena adesione ai principi e alle regole della protezione dati, che costituiscono un necessario presupposto per assicurare la tutela dei diritti e delle libertà fondamentali delle persone.

Nel corso di questi anni l'Autorità ha raccolto numerose istanze (reclami, segnalazioni e quesiti) in merito ad alcuni specifici profili relativi alla figura del RPD. Inoltre, la stessa interlocuzione – in frequenti casi, anche la mancata interlocuzione – con i RPD dei vari enti pubblici ha denotato significative problematicità circa il coinvolgimento e l'apporto che questa figura può dare ai titolari del trattamento in ambito pubblico.

È stata anche promossa, nel corso del 2019-2020, un'intensa attività ispettiva volta ad indagare i fenomeni di affidamento dell'incarico di RPD a società esterne, con particolare riferimento agli aspetti della numerosità degli incarichi accumulati da singole società e dei possibili conflitti di interessi dovuti alla sovrapposizione dei ruoli di RPD e di fornitori di servizi di carattere informatico.

Nell'ambito della complessiva analisi dell'attuazione delle norme del Regolamento dedicate al RPD, sono stati rivolti anche alcuni quesiti alle Autorità degli altri Stati membri dell'Unione europea, sotto forma di assistenza reciproca volontaria (ai sensi dell'art. 61 del Regolamento), al fine di comprendere se le medesime criticità siano state riscontrate anche in altri Paesi e quali iniziative, in proposito, tali Autorità abbiano intrapreso.

Infine, l'Autorità, dopo aver registrato lacune ed inesattezze nella comunicazione dei dati di contatto del RPD, prevista dall'art. 37, par. 7, del Regolamento effettuata in sede di prima applicazione della disposizione, ha altresì avviato una campagna volta ad ottenere la

regolarizzazione di tale adempimento, necessario per consentire all'Autorità, con la tempestività richiesta dalle singole circostanze, di stabilire un colloquio con i "punti di contatto" stabiliti presso le singole amministrazioni.

A fronte dei tanti impulsi in tal modo emersi, il Garante ritiene necessario fornire dei chiarimenti, al fine di rendere più effettiva ed efficace l'attività del RPD e di mettere il titolare del trattamento nelle migliori condizioni per assicurare il corretto trattamento dei dati personali.

In particolare, tale esigenza si rende necessaria per il settore pubblico, laddove la designazione del RPD rappresenta un obbligo, ai sensi dell'art. 37, par. 1, lett. a), del Regolamento.

Questa peculiarità ha fatto sì che, in molte realtà, tale onere generalizzato sia stato talvolta vissuto come un mero adempimento formale, senza comprendere adeguatamente l'importanza della figura in questione nel supporto e nella vigilanza sulla correttezza dei trattamenti di dati personali effettuati dal titolare. Ciò ha fatto sì che, una volta affidato l'incarico, in molte situazioni, non venisse prestata la dovuta attenzione ad aspetti quali il coinvolgimento del RPD, l'assegnazione di risorse sufficienti o l'attribuzione di ulteriori incarichi dalla dubbia compatibilità.

A distanza di circa tre anni dalla piena applicazione del Regolamento occorre ora superare queste incertezze: per questo il Garante ha deciso di adottare il presente documento *"Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico"*, con il quale intende fornire i chiarimenti agli interrogativi di maggior rilievo che sono stati posti all'attenzione dell'Autorità nel triennio appena trascorso e conseguentemente orientare i titolari del trattamento.

Il Documento di indirizzo viene adottato ai sensi dell'art. 57, par. 1, lett. b) e d), del Regolamento – concernenti, rispettivamente, i compiti di "[promuovere] la consapevolezza e [favorire] la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento" e di "[promuovere] la consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo agli obblighi imposti loro dal presente regolamento" – ma anche ai sensi dell'art. 154-bis, comma 1, lett. a), del Codice – concernente il potere di *"adottare linee guida di indirizzo riguardanti le misure organizzative e tecniche di attuazione dei principi del Regolamento, anche per singoli settori e in applicazione dei principi di cui all'articolo 25 del Regolamento"*.

A questo proposito, si precisa che il Documento di indirizzo recepisce, al suo interno, i chiarimenti già emanati con le citate *"Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico"* del 2017, che comunque rimangono anche quali indicazioni autonomamente reperibili.

In relazione ai singoli profili oggetto di trattazione, il Documento di indirizzo non fornisce indicazioni circa le conseguenze delle violazioni delle disposizioni normative suscettibili di condurre all'avvio del procedimento volto all'adozione dei provvedimenti correttivi e sanzionatori, ai sensi dell'art. 166 del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196). A questo proposito, resta fermo che l'accertamento di eventuali illiceità nelle condotte di titolari e responsabili del trattamento sarà oggetto di valutazione caso per caso, a seconda degli elementi che di volta in volta emergeranno nel corso delle singole istruttorie, al fine di riscontrare l'eventuale violazione degli artt. 37, 38 e 39 del Regolamento, oggetto di possibile applicazione della sanzione amministrativa ai sensi dell'art. 83, par. 4, lett. a), del medesimo Regolamento. In ogni caso, le indicazioni contenute nel Documento di indirizzo sono rivolte anche ai RPD, in quanto li impegnano nell'esecuzione dei compiti demandati loro dal Regolamento medesimo.

Per quanto riguarda il settore privato, date le sensibili differenze rispetto al mondo delle pubbliche amministrazioni e tenuto conto delle peculiarità che lo contraddistinguono – a partire

dalla circostanza che, ai sensi dell'art. 37, par. 1, lett. b) e c), del Regolamento la designazione del RPD diviene obbligatoria solo al ricorrere di alcune specifiche condizioni – si rinvia alle *"Faq sul Responsabile della Protezione dei dati (RPD) in ambito privato"* (pubblicate inizialmente il 26 marzo 2018, doc. *web* n. 8036793), che sono state oggetto di aggiornamento, da parte dell'Autorità, a fronte dei primi anni di applicazione del Regolamento e contestualmente all'adozione del presente provvedimento.

2. Una considerazione preliminare: il RPD quale “punto di contatto” per l’Autorità

L’art. 39, par. 1, lett. d) ed e), del Regolamento prevede che il RPD, tra i suoi compiti, cooperi con l’Autorità e funga da punto di contatto per questioni connesse ai trattamenti. Come indicato nelle Linee guida del WP29, in questo modo il RPD svolge un ruolo di “*facilitatore*”, in quanto facilita l’accesso, da parte dell’Autorità, ai documenti e alle informazioni necessarie “*per l’adempimento dei compiti attribuiti dall’articolo 57 nonché ai fini dell’esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi di cui all’articolo 58*” (par. 4.3, pp. 23-24).

Questo delicato compito carica ancor di più di significato l’obbligo per il titolare/responsabile del trattamento, stabilito dall’art. 38, par. 1, del Regolamento, di assicurarsi che il RPD sia “*tempestivamente e adeguatamente*” coinvolto in tutte le questioni riguardanti la protezione dei dati personali, (su questo specifico profilo, cfr. par. 8).

Ciò significa che, nell’attività di acquisizione di elementi da parte dell’Autorità nello svolgimento delle proprie funzioni, deve sempre essere garantito il supporto del RPD. Tale supporto è necessario:

- da un lato, al titolare/responsabile, al fine di individuare la documentazione e le informazioni corrette e pertinenti da fornire all’Autorità (sul punto, cfr. le difficoltà emerse nell’istruttoria che ha condotto all’adozione del provv. 17 dicembre 2020, n. 280, doc. web n. 9524175);
- dall’altro lato, all’Autorità stessa, al fine di agevolare l’attività istruttoria e consentire il tempestivo accertamento della conformità dei trattamenti indagati alla normativa in materia di protezione dei dati personali.

Per queste ragioni, in sede di istruttoria preliminare, le richieste di informazioni saranno tendenzialmente indirizzate anche al RPD, pur rimanendo l’onere di fornire riscontro (e la conseguente responsabilità dell’eventuale inadempimento) in capo al titolare/responsabile destinatario della comunicazione (cfr., ad esempio, l’art. 157 del Codice con riferimento alle richieste di informazioni, o l’art. 166, commi 5 e 6, del Codice con riferimento all’avvio del procedimento per l’adozione dei provvedimenti correttivi o sanzionatori).

A questo fine, risulta quindi essenziale che il titolare/responsabile del trattamento comunichi tempestivamente all’Autorità i dati esatti di contatto del RPD, ai sensi dell’art. 37, par. 7, del Regolamento, provvedendo al loro tempestivo aggiornamento, anche in caso di modifica dei dati o di sostituzione del soggetto designato (in tema di comunicazione dei dati di contatto all’Autorità, cfr. par. 7). Peraltro, la presenza di dati non esatti o non aggiornati presso l’Autorità potrebbe comportare l’inoltro di comunicazioni a soggetti che non sono (o non sono più) RPD, mettendoli in questo modo (impropriamente) a parte di informazioni riservate connesse all’esercizio delle funzioni istituzionali.

Infine, si invitano i titolari/responsabili in ambito pubblico a coinvolgere sistematicamente il proprio RPD anche in relazione ad altre attività espletate dall’Autorità quali accertamenti ispettivi (cfr. art. 158 del Codice), audizioni (cfr. art. 166, comma 6, del Codice), richieste di parere (cfr. art. 36, par. 4, del Regolamento, e art. 154, comma 5, del Codice) riunioni svolte a qualsiasi titolo. In questa sede, la presenza di una figura qualificata ed esperta in materia e che conosce nel dettaglio i trattamenti svolti presso il titolare/responsabile, è in grado di assicurare una più corretta e completa rappresentazione delle questioni trattate e delle eventuali iniziative da suggerire – pur rimanendo il potere decisionale in capo al titolare del trattamento.

Il medesimo invito a interpellare preliminarmente il proprio RPD vale, in modo particolare, in relazione a eventuali quesiti relativi a trattamenti posti sotto la loro gestione, in relazione ai quali il Garante, in generale, non è dotato di compiti consultivi, al di fuori da quelli espressamente previsti dal Regolamento o dalla legge. Ciò consentirà, infatti, al RPD di poter esercitare i compiti affidatigli dal Regolamento (a partire da quelli di consulenza di cui all'art. 39, par. 1, lett. a)), e all'amministrazione di trovare le risposte al proprio interno, nella massima valorizzazione dell'*accountability* di cui agli artt. 5, par. 2, e 24 del Regolamento. Qualora, comunque, l'ente ritenesse di doversi rivolgere all'Autorità, sarà opportuno che lo faccia solo per il tramite del proprio RPD, e solo dopo averne comunque acquisito il relativo parere, che dovrà essere allegato alla richiesta.

3. Obbligo di designazione

Disposizione di riferimento del Regolamento. Art. 37, par. 1: *"Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10".*

Cons. 91: *"[...] Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato [...]"*.

Riferimento nelle Linee guida del WP29: par. 2.1, pp. 6-12.

Ulteriore disposizione prevista dal Codice. Art. 2-sexiesdecies: *"Il responsabile della protezione dati è designato, a norma delle disposizioni di cui alla sezione 4 del capo IV del Regolamento, anche in relazione ai trattamenti di dati personali effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni"*.

Precedenti decisioni del Garante. *"Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico"*, 15 dicembre 2017 (doc. web n. 7322110); provv. 7 marzo 2019, *"Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario"* (doc. web n. 9091942); Relazione annuale 2019, par. 5.4 (pp. 89-91); provv. 17 dicembre 2020, n. 272 (doc. web n. 9557593); provv. 11 febbraio 2021, n. 54 (doc. web n. 9556625).

Questioni emerse. Al di là di autorità pubbliche o organismi pubblici, in relazione ai quali l'obbligo di designazione è stabilito in maniera chiara dalla lett. a) dell'art. 37, par. 1, del Regolamento, si è posto il dubbio circa i casi in cui tale designazione sia obbligatoria o meno, alla luce delle successive lett. b) e c), in relazione a soggetti privati che esercitano comunque compiti di interesse pubblico: è il caso, ad esempio, dei concessionari di pubblici servizi, o delle strutture sanitarie private.

Inoltre, per quanto concerne amministrazioni complesse (come i Ministeri), dotate di articolazioni territoriali oppure settoriali, ci si è domandato se fosse possibile designare più di un RPD, magari assegnandone uno per ciascuna di tali articolazioni.

Misure indicate. Preliminarmente, occorre ricordare che sussiste l'obbligo di designazione per tutti i soggetti pubblici, ai sensi della lett. a) dell'art. 37, par. 1, del Regolamento, quali, ad esempio: le amministrazioni dello Stato, anche con ordinamento autonomo, compresi gli istituti scolastici; 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 (cfr., a valenza meramente indicativa e non esaustiva, l'elenco di cui all'art. 1, comma 2, del d.lgs. 30 marzo 2001, n. 165).

Per quanto concerne, in generale, i soggetti privati che esercitano funzioni pubbliche, pur essendo l'obbligo di designazione del RPD rimesso a una valutazione che tenga conto degli elementi di cui alle lett. b) e c) dell'art. 37, par. 1, del Regolamento, alla luce delle indicazioni contenute nelle Linee guida del WP29, è comunque fortemente raccomandato individuare ed investire una figura dell'incarico di RPD, tenendo conto, tra le altre cose, che le caratteristiche dei trattamenti da costoro svolti sono assimilabili a quelli effettuati da soggetti propriamente pubblici, stante la medesima riconducibilità a compiti di interesse pubblico. In ogni caso, è altamente probabile che, in tali situazioni, i requisiti di cui alle lett. b) e c) dell'art. 37, par. 1, del Regolamento tendenzialmente vengano soddisfatti, per cui si ricadrebbe conseguentemente nell'obbligo di designazione.

È il caso, ad esempio, delle società concessionarie dei servizi di trasporto pubblico locale, di gestione delle autolinee pubbliche o di raccolta dei rifiuti, allorché utilizzano sistemi che comportano il trattamento, su larga scala, di dati di dipendenti e utenti, associato a un monitoraggio regolare o sistematico: si pensi ai dispositivi di geolocalizzazione dei veicoli impiegati nel servizio, alle forme di tracciamento dei titoli di viaggio o ai *call center* per la gestione delle telefonate dell'utenza. Per quanto concerne, nello specifico, il servizio di trasporto pubblico, si tenga peraltro conto che l'utenza è composta anche da interessati caratterizzati da una particolare situazione di vulnerabilità (come minori o persone disabili), con conseguente trattamento di categorie particolari di dati personali.

Per quanto concerne lo specifico ambito sanitario, posto che le Aziende sanitarie appartenenti al Servizio sanitario nazionale sono obbligate alla designazione in quanto si tratta di organismi pubblici, anche ospedali privati, case di cura o Residenze sanitarie assistenziali (RSA) si devono ritenere, in via generale, sottoposti all'obbligo di designazione, trattando dati sulla salute su larga scala (art. 37, par. 1, lett. c), del Regolamento).

Quanto, poi, al singolo professionista sanitario che operi in regime di libera professione a titolo individuale, si fa presente che lo stesso non è tenuto alla designazione di tale figura con riferimento allo svolgimento della propria attività, in quanto, secondo quanto indicato nel cons. 91 del Regolamento, i trattamenti dallo stesso effettuati non rientrano tra quelli su larga scala. Anche farmacie, parafarmacie, e aziende ortopediche e sanitarie, se non effettuano trattamenti di dati personali su larga scala, non sono obbligati a designare il RPD.

Infine, per quanto concerne il "numero" di RPD di cui si può avvalere un'amministrazione, 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.

Ciò significa che, presso amministrazioni particolarmente complesse, come i Ministeri, è in ogni caso necessario che venga individuato un solo RPD, in corrispondenza dell'unicità dell'ente quale titolare del trattamento, i cui dati di contatto dovranno essere pubblicati e comunicati all'Autorità ai sensi dell'art. 37, par. 7, del Regolamento, in quanto egli rappresenta il punto di

contatto unico, sia per l'Autorità che per gli interessati, pur potendosi avvalere di referenti allocati presso altre articolazioni che gli forniscano il supporto opportuno.

3.1. Designazione di RPD interno nelle more della conclusione del procedimento di affidamento dell'incarico a RPD esterno

Precedente decisione del Garante. Provv. 1° ottobre 2020, n. 173 (doc. web n. 9483375).

Questione emersa. Si è posta la questione se, a seguito della scadenza dell'incarico di un RPD (ad esempio, per cessazione del contratto con un RPD esterno o per collocamento a riposo di un RPD interno), e in attesa della conclusione della procedura di affidamento dell'incarico ad un nuovo RPD (perlopiù esterno), l'ente pubblico possa attendere l'esito di tale procedura oppure, nelle more, sia tenuto a designare, anche temporaneamente, un RPD (eventualmente interno) per il tempo necessario a colmare questo periodo di *vacatio*.

Misure indicate. In questi casi, nelle more della selezione del nuovo RPD esterno, in ossequio al principio generale di continuità dell'azione amministrativa che è strettamente correlato a quello di buon andamento dell'azione stessa, al fine di non violare l'art. 37, par. 1, del Regolamento, l'amministrazione pubblica è comunque tenuta a individuare temporaneamente, al proprio interno, un dirigente/funziionario da designare interinalmente in questo ruolo.

Tale soggetto interno deve essere in possesso dei requisiti richiesti dal Regolamento e, qualora questo abbia già un incarico dirigenziale all'interno dell'organizzazione del titolare, ciò non dovrebbe comportare la sottrazione del tempo necessario allo svolgimento dei compiti assegnati al RPD, né dovrebbe dare luogo a una situazione di conflitto di interessi, qualora ad esempio partecipi alla definizione delle finalità o modalità dei trattamenti di dati personali effettuati dal titolare.

Posto, pertanto, l'obbligo per ogni ente pubblico di essere dotato di un RPD nel pieno delle sue funzioni, spetta a ciascun ente pubblico, in conformità al principio di *accountability*, ogni valutazione in merito alla scelta della figura da individuare quale RPD, tenuto in ogni caso conto che tale particolare situazione di transitorietà rappresenta un elemento utile nella valutazione della sussistenza di un effettivo rischio di conflitto di interessi in cui potrebbe incorrere la risorsa interna temporaneamente designata.

Restano in ogni caso fermi gli obblighi di pubblicazione dei dati di contatto del RPD e di comunicazione degli stessi a questa Autorità, ai sensi dell'art. 37, par. 7, del Regolamento, anche con riferimento alla figura nominata in via temporanea.

4. Designazione di un unico RPD per conto di più soggetti pubblici

Disposizione di riferimento del Regolamento. Art. 37, par. 3: *"Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione"*.

Riferimento nelle Linee guida del WP29: par. 2.3, pp. 13-14; par. 3.2, pp. 18-19.

Precedenti decisioni del Garante. Relazione annuale 2018, par. 5.4.3 (pp. 84-85); provv. 7 marzo 2019, *"Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario"* (doc. web n. 9091942).

Questione emersa. In ambito pubblico, considerato che il titolare del trattamento può presentare una struttura organizzativa e una dimensione limitate, che incidono sulla sua concreta capacità (soprattutto in termini di risorse) di dotarsi di una figura esclusivamente dedicata a svolgere l'incarico di RPD (si pensi ai tanti Comuni con una popolazione numericamente ridotta, oppure agli Istituti scolastici), si riscontra un ampio ricorso alla semplificazione introdotta dall'art. 37, par. 3, del Regolamento, che consente a questi soggetti di individuare, per il ruolo di RPD, una figura "in comune", in questo modo abbattendo i costi e semplificando le procedure di selezione.

Lo svolgimento della funzione di RPD per conto di più titolari deve necessariamente tenere conto della possibilità di consentire, alla figura incaricata, di prestare il necessario supporto a tutti i suddetti titolari (anche in termini di tempo e disponibilità da dedicare loro) e di assolvere in maniera adeguata ai compiti assegnatigli dall'art. 39 del Regolamento.

Tale circostanza deve essere oggetto di valutazione particolarmente attenta nei seguenti casi: quando i trattamenti effettuati dai titolari hanno ad oggetto dati personali di particolare delicatezza, magari anche su larga scala (si pensi alle Aziende sanitarie, che trattano dati relativi alla salute riferiti a un numero significativo di assistiti, in un contesto tecnologico in continuo cambiamento); quando i titolari che si avvalgono del medesimo RPD operano in contesti molto differenti tra loro (ad es., Comuni e Istituti scolastici oppure anche soggetti privati), per cui anche i trattamenti effettuati differiscono in maniera rilevante tra loro, richiedendo al RPD un maggiore impegno nell'approfondimento delle diverse peculiarità.

Misure indicate. Qualora più soggetti pubblici intendano avvalersi di un unico RPD, occorre che, nel rispetto del principio di responsabilizzazione (artt. 5, par. 2, e 24 del Regolamento), essi effettuino un'adeguata valutazione che tenga in considerazione tutte le implicazioni tecniche, giuridiche e pratiche di tale decisione.

A questo proposito, al fine di prevenire le richiamate criticità, e quindi di assicurare l'efficace svolgimento dei propri compiti, i soggetti pubblici potrebbero:

- a) costituire un gruppo di collaboratori a supporto del RPD designato in comune;

- b) definire preventivamente la percentuale del tempo lavorativo destinata all'attività da svolgere nei confronti di ciascun titolare del trattamento che ha designato il medesimo RPD;
- c) individuare, per ciascun singolo titolare del trattamento, uno specifico referente cui il RPD possa rivolgersi;
- d) in sede di procedura di selezione, chiedere ai candidati all'incarico di RPD, quale elemento per verificare che non sussistano situazioni di potenziale incompatibilità, di specificare nei confronti di quanti altri titolari sia svolta già la medesima funzione, eventualmente indicando anche le tipologie di enti pubblici (ad es., quanti Comuni, quanti Istituti scolastici, quante Aziende fornitrici di servizi pubblici, ecc.).

4.1. Comunicazione dei dati di contatto da parte di ciascun titolare in presenza di un RPD selezionato da più titolari

Altra disposizione di riferimento del Regolamento. Art. 37, par. 7: *"Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo".*

Riferimento nelle Linee guida del WP29: par. 2.6, pp. 16-17.

Questione emersa. In alcuni casi in cui un unico RPD veniva selezionato, da parte di un organismo associativo, per conto dei titolari del trattamento associati tra di loro in ragione di dimensioni e risorse limitate, si è riscontrato che la comunicazione dei dati di contatto del RPD all'Autorità veniva effettuata solo da parte soggetto associato anziché da ciascun singolo titolare del trattamento. Tale eventualità si è verificata di frequente nell'ipotesi di Unione di Comuni, ove la richiamata comunicazione veniva effettuata da parte della sola Unione, anziché da parte di ciascun singolo Comune che la compone.

Al contrario, si rileva che la comunicazione dei dati di contatto del RPD all'Autorità, come anche la loro pubblicazione, sono attività necessarie al fine di garantire all'Autorità e agli interessati la possibilità di contattare il RPD in modo facile e diretto: per tale motivo la citata disposizione, stante la possibilità di selezione di un unico RPD per conto di una pluralità di enti pubblici, non fa venire meno il dovere, da parte di ciascun titolare del trattamento, di pubblicare i dati e di comunicarli all'Autorità. Peraltro, il soggetto pubblico che associa tali enti (nell'esempio richiamato, l'Unione di Comuni) è un soggetto autonomo che a sua volta può essere titolare di trattamenti, in base a quanto stabilito dalla legge (cfr., nel caso delle Unioni di Comuni, l'art. 32 del d.lgs. 18 agosto 2000, n. 267), e per questo deve avere un suo RPD (eventualmente anche distinto da quello dei Comuni che ne fanno parte).

Misure indicate. In questi casi, dunque, ciascun ente pubblico che sia titolare del trattamento è tenuto ad effettuare la comunicazione dei dati di contatto del RPD all'Autorità, nonché la pubblicazione degli stessi sul proprio sito *web*. Pertanto nel caso di Unione di Comuni che, per effetto del conferimento di tale funzione da parte dei Comuni che la compongono, individui un RPD unico per i medesimi Comuni, ciascuno di tali Comuni è tenuto a effettuare i

richiamati adempimenti. Rimane fermo che il soggetto associativo, qualora sia a sua volta titolare di trattamenti di dati personali (ad esempio, l'Unione di Comuni cui è delegato l'esercizio di funzioni in forma associata), sarà tenuto a designare un proprio RPD e a svolgere i medesimi adempimenti (pubblicazione e comunicazione dei dati di contatto all'Autorità).

5. Qualità professionali e possesso di titoli

Disposizione di riferimento del Regolamento. Art. 37, par. 5: *"Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39".*

Riferimento nelle Linee guida del WP29: par. 2.5, pp. 14-16.

Precedenti decisioni del Garante. Nota del 28 luglio 2017, *"Quesiti in materia di certificazione delle competenze ai fini della prestazione di consulenza in materia di protezione dei dati personali"* (doc. web n. 7057222); *"Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico"*, 15 dicembre 2017 (doc. web n. 7322110).

Decisioni di altri organismi: sentenza del Tar Friuli-Venezia Giulia, sez. I, del 13 settembre 2018, n. 287; atto di segnalazione dell'Autorità garante della concorrenza e del mercato AS1636 del 2 gennaio 2020.

Questione emersa. In alcuni casi, è stato riscontrato che, in ambito pubblico, il titolare del trattamento, per selezionare una figura dotata delle competenze necessarie, ha richiesto che il candidato fosse in possesso di titoli specifici, come ad esempio uno specifico titolo di studio (perlopiù la laurea in giurisprudenza), l'iscrizione ad un determinato albo professionale (spesso quello di avvocato) o particolari tipologie di certificazione (come le cc.dd. certificazioni volontarie).

I requisiti in tal modo richiesti non sono stabiliti dal Regolamento o da altre disposizioni normative, e il loro eventuale possesso non equivale, di per sé, a un'abilitazione allo svolgimento del ruolo del RPD, né può sostituire *in toto* la valutazione del soggetto pubblico nell'analisi del possesso dei requisiti del RPD necessari per lo svolgimento dei suoi compiti. Pertanto, escludere alcuni candidati solo perché privi di determinati titoli potrebbe apparire sproporzionato e discriminatorio, tenuto conto che tali requisiti, di per sé, non sono necessariamente in grado di dimostrare il possesso delle competenze tecniche per lo svolgimento adeguato della funzione di RPD (ad esempio, l'avvocato che non si è mai occupato di protezione dei dati personali), potendo, invece, escludere in modo ingiustificato dalla competizione soggetti ugualmente esperti della materia, come potrebbero esserlo soggetti non iscritti all'albo degli avvocati che dimostrino di aver completato la propria preparazione anche sul versante giuridico o di avere una comprovata esperienza in materia di protezione dei dati personali.

Misure indicate. Preliminarmente, si rende necessario che l'ente pubblico valuti le qualità professionali, le conoscenze specialistiche e l'esperienza in materia di protezione dei dati personali in capo alla figura da incaricare quale RPD, tenendo conto dei trattamenti che effettua, prestando particolare cura, ad esempio, alla complessità dei trattamenti stessi, alla qualità e quantità di dati personali trattati, all'esistenza di trasferimenti sistematici ovvero occasionali di dati personali al di fuori dell'Unione europea. Ciò comporta che, in ambito pubblico, il RPD debba

certamente conoscere la normativa e le prassi nazionali ed europee in materia di protezione dei dati (a partire da un'approfondita conoscenza del Regolamento), nonché possedere un'adeguata conoscenza anche delle norme e procedure amministrative che caratterizzano lo specifico settore, in quanto la liceità del trattamento dei dati personali in questo ambito dipende dalla corretta applicazione delle regole di volta in volta previste dalla disciplina di settore.

Per quanto concerne la conoscenza di norme e prassi in materia di protezione dei dati personali, essa può essere dimostrata, in primo luogo, attraverso una documentata esperienza professionale e/o anche attraverso la partecipazione ad attività formative specialistiche (ad esempio, master, corsi di studio e professionali, specie se risulta documentato il livello di acquisizione delle conoscenze). Rientra in questo contesto anche la certificazione volontaria acquisita sulla base della norma tecnica italiana UNI 11697 *"Attività professionali non regolamentate – Profili professionali relativi al trattamento e alla protezione dei dati personali – Requisiti di conoscenza, abilità e competenza"*, che può rappresentare un elemento utile di valutazione della preparazione del candidato, ma non un'abilitazione di per sé aprioristica.

Analogamente, la conoscenza specialistica sarà dimostrata dalle attività, dalle esperienze lavorative e professionali svolte, risultanti, ad esempio, dal *curriculum* e dalle autocertificazioni presentate. Particolare valore potrà assumere l'eventuale esperienza del candidato in organizzazioni simili a quella del titolare.

In tale contesto, preme in ogni caso evidenziare che la competenza a ricoprire il ruolo di RPD non può essere astrattamente riconosciuta in capo ad una qualsiasi figura per effetto del semplice possesso di specifici titoli (laurea, iscrizione ad un albo professionale, certificazione). Il titolare del trattamento è infatti tenuto a valutare nel complesso gli elementi previsti dall'art. 37, par. 5, del Regolamento e, qualora intenda richiedere un titolo di studio specifico, è chiamato a tenere in dovuta considerazione la proporzionalità tra quanto richiesto e la complessità del compito da svolgere nel caso concreto, comprovando le proprie scelte ai sensi degli artt. 5, par. 2, e 24 del Regolamento, a partire da un'adeguata motivazione nel provvedimento di assegnazione formale dell'incarico.

Pertanto, ne discende che, al momento della definizione dei requisiti in base ai quali individuare il soggetto da incaricare quale RPD, l'ente pubblico deve evitare restrizioni all'accesso alle selezioni che possano risultare sproporzionate e ingiustificate rispetto alla figura ritenuta necessaria, ma tenere in debita considerazione l'attinenza e la proporzionalità tra quanto richiesto (le qualità professionali di cui all'art. 37, par. 5, del Regolamento) e la complessità del compito da svolgere nel caso concreto (come il contesto in cui il RPD sarà chiamato ad operare o le caratteristiche dei trattamenti effettuati dall'ente designante).

6. Questioni attinenti alla designazione di un RPD esterno

Disposizione di riferimento del Regolamento. Art. 37, par. 6: *"Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi"*.

Riferimento nelle Linee guida del WP29: par. 2.5, pp. 14-16.

6.1. Allineamento tra contratto di servizi, atto di designazione e pubblicazione/comunicazione al Garante

Altra disposizione di riferimento del Regolamento. Art. 39, par. 1: *"Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; d) cooperare con l'autorità di controllo; e e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione"*.

Precedente decisione del Garante. *"Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico"*, 15 dicembre 2017 (doc. web n. 7322110).

Questioni emerse. Nel corso di alcune istruttorie condotte dall'Autorità, è emerso che, con riferimento alla scelta di un RPD esterno, gli atti adottati al fine di rendere operativa tale figura non risultano sempre pienamente allineati tra loro, per cui le indicazioni in ciascuno contenute risultano non univoche. In particolare, in queste situazioni si è talora riscontrato che: l'offerta per il servizio viene effettuata da società che indicano la persona fisica da individuare come RPD; tale offerta, in caso di affidamento alla suddetta società, diviene contratto di servizio, per effetto dell'accettazione operata con apposita determinazione dirigenziale dell'ente; l'atto di designazione (che, ad esempio nei Comuni, generalmente assume la forma di decreto sindacale) avviene nei confronti della persona fisica indicata, ma con l'utilizzo di forme ambigue circa il ruolo assunto dalla società che aveva partecipato alla gara.

A ciò si aggiunga che il rapporto tra l'amministrazione e la società in questione viene talvolta formalizzato mediante accordo ai sensi dell'art. 28 del Regolamento per lo svolgimento di taluni compiti, tra cui il supporto tecnico e organizzativo al RPD medesimo o attività di assistenza diretta nei confronti del titolare, sempre nel settore della protezione dei dati personali (come, ad esempio, in riferimento alla valutazione d'impatto sulla protezione dei dati) o specifici compiti quali, ad esempio, la fornitura di piattaforme tecnologiche o specifiche funzionalità (registro delle attività di trattamento, erogazione di eventi formativi, predisposizione di informative, ecc.).

Il quadro descritto determina una certa confusione circa i ruoli assunti dai soggetti coinvolti nel trattamento e nell'affidamento del servizio di RPD, con una sovrapposizione di figure, compiti e atti che rende incoerente, macchinosa e poco trasparente l'instaurazione del relativo rapporto.

Misure indicate. In via preliminare, occorre precisare che, 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 potrà costituire parte integrante dell'apposito contratto di servizi (ad esempio, come suo allegato).

Indipendentemente dalla natura e dalla forma dell'atto utilizzato, è necessario che nello stesso sia individuata, in maniera inequivocabile, la persona fisica o giuridica che opererà come RPD, riportandone espressamente le generalità (o i dati societari, in caso di persona giuridica), i compiti 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 nel tempo 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 Regolamento, anche mediante rinvio agli esiti delle procedure di selezione. La specificazione dei criteri utilizzati nella valutazione compiuta dall'ente nella scelta di tale figura, oltre a essere indice di trasparenza e di buona amministrazione, costituisce anche elemento di valutazione del rispetto del principio di *accountability*.

Tutto ciò premesso, venendo alle criticità evidenziate, si rende necessario che:

- a) il soggetto individuato quale RPD, che si tratti di persona fisica o giuridica, sia il medesimo indicato in tutti gli atti che contribuiscono a perfezionare il processo di designazione, ciò vale sicuramente per: la domanda di partecipazione ad una procedura selettiva; il contratto di servizio (nel caso di affidamento ad un soggetto esterno); l'atto di designazione (con il quale effettivamente viene individuato e investito il soggetto del ruolo e dei compiti del RPD); le informazioni contenenti i relativi dati di contatto, da pubblicare sul sito *web* dell'ente e da comunicare all'Autorità;

- b) se il soggetto individuato quale RPD è una persona giuridica, questa deve indicare, a sua volta, il referente persona fisica; a questo proposito, è opportuno che essa sia indicata, già in fase di procedura di selezione e in ciascuno degli atti summenzionati, e che ogni variazione che dovesse riguardare quest'ultima sia coerentemente riportata negli stessi e comunicata all'Autorità (mediante l'apposita procedura disponibile sul sito del Garante: cfr. par. 7);
- c) l'individuazione di eventuali figure, sia interne che esterne all'ente, di supporto al RPD, avvenga in maniera chiara e trasparente, da parte dell'amministrazione, eventualmente anche all'interno dell'atto di designazione del RPD stesso. Tali figure di supporto, ai soli fini dello svolgimento dei compiti propri del RPD, possono ricevere istruzioni solo da quest'ultimo: pertanto, a questo specifico fine, non possono ricevere istruzioni dal titolare del trattamento, né, tantomeno, possono essere legate a quest'ultimo da un rapporto instaurato ai sensi dell'art. 28 del Regolamento;
- d) ulteriori figure che forniscono servizi al titolare del trattamento, in qualità di responsabili del trattamento con i quali è instaurato un rapporto ai sensi dell'art. 28 del Regolamento, non svolgano altresì compiti di RPD o di supporto al RPD, stante l'autonomia dell'azione di quest'ultimo – considerato che gli stessi rapporti instaurati con i responsabili del trattamento sono sottoposti alla vigilanza del RPD, ai sensi dell'art. 39, par. 1, lett. b), del Regolamento.

6.2. Pluralità di enti pubblici per conto dei quali viene svolto l'incarico e pluralità di servizi forniti anche al medesimo titolare

Precedenti decisioni del Garante. *"Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico"*, 15 dicembre 2017 (doc. web n. 7322110); Relazione annuale 2019, par. 4.9 (pp. 80-81).

Questione emersa. Dagli accertamenti ispettivi condotti è emerso che alcune società svolgono incarichi di RPD per conto di numerosi soggetti pubblici (nell'ordine delle centinaia), spesso anche variamente dislocati sull'intero territorio nazionale. Oltre all'incarico di RPD, è emerso che tali società svolgono anche altri incarichi che pur non essendo, in generale, incompatibili con il ruolo di RPD (ad esempio, quello di referente nell'ambito della sicurezza del lavoro) potrebbero comunque rendere difficile lo svolgimento di tutti i compiti affidati, soprattutto quando queste società operano con risorse non adeguate, incidendo anche sulla credibilità della qualità del lavoro svolto come RPD.

A questo proposito, si sono riscontrate situazioni in cui queste società indicano, quale referente persona fisica per conto dei vari "clienti", sempre i medesimi collaboratori, affiancandoli con una squadra composta da un numero molto esiguo di unità. Peraltro, in alcuni casi, questi non sono nemmeno deputati allo svolgimento esclusivo di funzioni di supporto al RPD, ma svolgono anche altri incarichi (compiti di amministrazione, formazione alla sicurezza sul lavoro, ecc.; per quanto concerne specifiche situazioni di incompatibilità e conflitto di interessi, cfr. par. 10).

La numerosità dei clienti per i quali tali società svolgono il ruolo di RPD, considerato l'esiguo numero di risorse umane, materiali e temporali impiegate in rapporto alla complessità e alla numerosità dei compiti affidati, fa sorgere dei dubbi sul fatto che le modalità di svolgimento del ruolo di RPD possano ritenersi effettivamente adeguate a fornire un efficace supporto a ciascun titolare per lo svolgimento dei compiti previsti dall'art. 39 del Regolamento (oltre che a fungere quale punto di contatto per gli interessati, ai sensi dell'art. 38, par. 4, del Regolamento). Le stesse perplessità emergono anche nelle ipotesi in cui una medesima figura che rivesta il ruolo di RPD sia chiamata, per conto anche del medesimo soggetto pubblico, a svolgere ulteriori incarichi.

Misure indicate. Posta la libertà di ciascun soggetto di organizzare la propria attività di impresa (e fatto salvo quanto detto al par. 10.2 circa l'organizzazione societaria), rimane il fatto che gli enti pubblici, nel momento in cui decidono di affidare l'incarico di RPD a un soggetto esterno alla propria struttura, al fine di prevenire la possibilità di ricevere una assistenza inadeguata, dovrebbero poter tenere in considerazione, ad esempio, i seguenti elementi:

- a) il numero di incarichi già ricoperti dalla società o dal professionista al quale si intende affidare l'incarico;
- b) l'eventuale specializzazione in ragione delle particolari tipologie di trattamenti effettuati dai soggetti per i quali tale soggetto svolge il ruolo di RPD (ad esempio, il fatto che si tratti prevalentemente di Comuni, o di Istituti scolastici, o di Aziende sanitarie, o di società commerciali, ecc.);
- c) in caso di società, la disponibilità di adeguate risorse a sostegno del referente persona fisica, compresa la possibilità di ricorrere, se del caso, a collaboratori in possesso di particolari competenze (cfr. par. 9).

Le indicazioni di cui sopra non hanno valore assoluto ma costituiscono, nel loro complesso, elementi di valutazione da tenere in attenta considerazione in fase di selezione.

Inoltre, ciascuna amministrazione dovrebbe valutare l'opportunità di individuare, al proprio interno, una figura di riferimento per il RPD esterno, con il quale quest'ultimo possa interloquire con costanza, al fine di consentirgli una più rapida e completa acquisizione di tutti gli elementi di contesto necessari per lo svolgimento dei suoi compiti e per facilitargli l'interazione con le strutture interne dell'ente.

6.3. Individuazione, all'interno del RPD persona giuridica, del referente persona fisica

Decisione di altro organismo: sentenza del Tar Puglia – Lecce, sez. III, del 13 settembre 2019, n. 1468.

Questione emersa. Sono emersi dubbi in ordine alla legittima possibilità che la persona giuridica candidata ad assumere l'incarico di RPD per conto di una pubblica amministrazione possa avvalersi di un referente persona fisica che non sia un dipendente della società medesima, e quindi sia esterno al suo organico.

Misure indicate. Preliminarmente, come indicato nelle Linee guida del WP29, deve essere chiarito che il referente persona fisica deve essere anch'egli in possesso di tutti i requisiti stabiliti dal Regolamento, compresi i requisiti professionali di cui all'art. 37, par. 5.

Ciò posto, si ritiene che obbligare una persona giuridica, che intenda candidarsi a rivestire l'incarico di RPD presso un ente pubblico, ad indicare quale referente persona fisica esclusivamente un proprio dipendente, escludendo così rapporti diversi da quello di subordinazione, impedisce a tutta una serie di realtà (quali società tra professionisti e studi professionali associati, o anche solo organizzazioni che abbiano stipulato un contratto di opera intellettuale con un professionista esterno) a prendere parte a procedure di affidamento del servizio in questione, senza che tale impedimento abbia alcun aggancio nel Regolamento, dove non è presente alcuna disposizione che richieda la sussistenza di un siffatto rapporto di subordinazione.

A questo proposito, nonostante si riscontrino dei primi orientamenti giurisprudenziali difformi, si ritiene che le Linee guida del WP29, laddove parlano di "appartenenza" della persona fisica alla persona giuridica, non intendono fornire a tale concetto alcuna precisa connotazione giuridica (probabilmente, anche al fine di rispettare l'autonomia dei singoli ordinamenti nazionali nella disciplina dei rapporti di lavoro). Infatti, le Linee guida, nella versione originale in lingua inglese, fanno riferimento a *"each member of the organisation exercising the functions of a DPO"*, utilizzando quindi una locuzione che rimanda ad un mero coinvolgimento delle persone fisiche preposte, senza che da ciò si possa dedurre la necessaria sussistenza di un vincolo di dipendenza parificabile ad un rapporto di lavoro subordinato (come, ad esempio, quello di cui all'art. 2094 c.c.).

Conseguentemente, si ritiene che il referente persona fisica indicato dalla persona giuridica non debba necessariamente essere un suo dipendente, e quindi non debba obbligatoriamente trovarsi in un rapporto di subordinazione, a nulla rilevando, ai fini dell'applicazione del Regolamento, il tipo di rapporto che lega la persona giuridica designata con il referente persona fisica. Deve, in ogni caso, sussistere un rapporto giuridico che fornisca prova della sussistenza di un legame valido, efficace e stabile e legittimi tale indicazione nei confronti dell'ente pubblico aggiudicante.

Tutto ciò considerato, deve in ogni modo essere sempre assicurata la massima e preventiva correttezza e trasparenza, da parte della persona giuridica che intende essere designata, nei confronti dell'ente affidante. Pertanto, nulla osta e, anzi, potrebbe essere considerata una buona pratica che l'ente committente richieda alle società candidate per l'incarico di RPD adeguate informazioni, eventualmente comprovate da idonea documentazione, circa la persona fisica da indicare come referente come, ad esempio:

- a) i dati identificativi;
- b) il possesso dei requisiti di cui all'art. 37, par. 5, del Regolamento;
- c) l'assicurazione che tale persona fisica non abbia già un numero di incarichi che ne rendano difficoltoso l'adempimento (ad esempio, indicando il numero di incarichi già rivestiti);
- d) il tipo di rapporto contrattuale intrattenuto.

Sempre al fine di assicurare la massima trasparenza, l'ente committente potrebbe valutare l'opportunità di inserire, all'interno del contratto, una clausola che obblighi la persona

giuridica affidataria a comunicargli qualsiasi variazione, intervenuta in sede di esecuzione, riguardante il referente persona fisica previamente individuato, al fine di consentire al titolare del trattamento di verificare che il RPD garantisca il mantenimento, nel tempo, dell'effettivo possesso dei requisiti richiesti.

6.4. Durata dell'incarico

Altra disposizione di riferimento del Regolamento. Art. 38, par. 3: *"Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento".*

Cons. 97: *"[...] Tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente".*

Decisione di altro organismo: delibera dell'Autorità nazionale anticorruzione n. 421 del 13 maggio 2020.

Questione emersa. Sono state riscontrate situazioni in cui la durata dell'incarico di RPD assegnato a un soggetto esterno all'amministrazione era strettamente legata alla durata del mandato del vertice della medesima (come, ad esempio, il Sindaco di un Comune).

A questo proposito, si rileva che il RPD deve svolgere la propria funzione in maniera indipendente rispetto alle decisioni adottate dal legale rappresentante del titolare del trattamento, mentre un legame in tal modo instaurato rischia di creare un rapporto su base fiduciaria, che può minare la separazione delle competenze e l'autonomia del RPD, creando una soggezione di fatto fra organo politico e soggetto di consulenza/sorveglianza.

Misure indicate. La durata del contratto di servizi deve tendenzialmente essere tale da consentire al RPD di poter impostare, in un periodo non breve, le attività necessarie per rendere conformi al Regolamento i trattamenti effettuati dal titolare che lo ha incaricato. Spetta ovviamente a ciascun ente pubblico valutare la congruità della durata rispetto alle caratteristiche dell'amministrazione (dimensioni, risorse a disposizione, ecc.) e a quelle dei trattamenti svolti (complessità, qualità e quantità dei dati personali trattati, ecc.): ma, in linea di massima, si ritiene che un periodo congruo per la durata dell'incarico possa essere stimato intorno ai tre anni, al fine di dare al RPD il tempo necessario per poter conoscere adeguatamente l'organizzazione dell'ente e attuare le misure necessarie a garanzia dei diritti degli interessati.

Ciò posto, nello stabilire la durata del contratto con il RPD esterno, l'ente pubblico, pur all'interno di una sfera di discrezionalità riguardo alle scelte organizzative, non può affidarsi a criteri che possano essere sintomatiche di un rapporto non improntato all'autonomia di azione

del RPD (come, ad esempio, lo stretto collegamento dell'incarico di RPD con il mandato di un organo direttivo dell'ente medesimo).

Infine, in quest'ottica, si richiamano le amministrazioni a prestare attenzione a quanto sostenuto dall'Autorità nazionale anticorruzione, a fini di rispetto della disciplina in materia di contratti pubblici, sulla necessità che l'affidamento dei contratti aventi ad oggetto il servizio di protezione dei dati personali di importo inferiore alle soglie comunitarie debba avvenire nel rispetto del principio di rotazione.

6.5. Remunerazione

Questioni emerse. Sono state rappresentate all'Autorità situazioni in cui bandi di gara per l'affidamento all'esterno del servizio di RPD prevedevano compensi estremamente bassi nell'ordine delle poche centinaia di euro, avvalendosi del criterio di aggiudicazione basato sul prezzo più basso di cui all'art. 95 del d.lgs. 18 aprile 2016, n. 50.

Nel corso dell'attività ispettiva sono emerse anche realtà peculiari in cui una società consortile, che già offre agli enti pubblici consorziati servizi a fronte del versamento di una quota annuale di partecipazione al consorzio, si è proposta, nei confronti dei medesimi enti, di fornire loro il servizio di RPD in forma gratuita. Questa scelta sarebbe motivata dalle garanzie offerte dalla propria "società partecipata" di riferimento, oltre che da evidenti ragioni di contenimento dei costi, tenuto peraltro conto che questo fenomeno si è sviluppato nelle aree del Paese più in difficoltà sotto il profilo economico e finanziario.

In proposito, si ritiene che l'eccessivo abbassamento della remunerazione per la fornitura del servizio di RPD abbia un duplice effetto negativo: da una parte, quello di consentire l'aggiudicazione in favore di candidati che, nonostante quanto previsto dall'art. 37, par. 5, del Regolamento, non abbiano una formazione specifica idonea allo svolgimento dei delicati compiti che spettano al RPD; dall'altra, quello di spingere i soggetti affidatari, per conseguire una remunerazione adeguata, ad accumulare un elevato numero di incarichi, con la conseguenza di non riuscire ad offrire un servizio efficace a ciascuno dei propri clienti (sul punto, cfr. le considerazioni riportate nel par. 6.2).

Misure indicate. Come per quanto detto in relazione alla durata del contratto, anche nella determinazione del compenso l'ente pubblico affidante, pur tenendo in adeguato conto le risorse a disposizione e la situazione organizzativa, dovrebbe effettuare valutazioni di congruità della cifra da stabilire, al fine di investire un RPD che svolga i propri compiti in maniera efficace.

In questa prospettiva, si invitano gli enti pubblici, nel momento della definizione dei criteri di aggiudicazione del servizio di RPD, a considerare di privilegiare la scelta del criterio dell'offerta economicamente più vantaggiosa, in coerenza con la preferenza accordata dall'art. 95 del d.lgs. 50/2016 e affermata dall'Adunanza plenaria del Consiglio di Stato (sent. 21 maggio 2019, n. 8), nonché in linea con le indicazioni fornite dall'Autorità nazionale anticorruzione. Infatti, come sancito dal richiamato orientamento giurisprudenziale, *"nell'ambito della generale facoltà discrezionale nella scelta del criterio di aggiudicazione, a sua volta insita nell'esigenza di rimettere all'amministrazione la definizione delle modalità con cui soddisfare nel miglior modo*

l'interesse pubblico sotteso al contratto da affidare, le stazioni appaltanti sono nondimeno vincolate alla preferenza accordata dalla legge a criteri di selezione che abbiano riguardo non solo all'elemento prezzo, ma anche ad aspetti di carattere qualitativo delle offerte" (cons. 8). Nel caso di specie, gli aspetti qualitativi sono direttamente collegati anche alla valutazione delle qualità professionali di cui all'art. 37, par. 5, del Regolamento: pertanto, le pubbliche amministrazioni dovranno temperare in maniera congrua e proporzionata le esigenze di razionalizzazione della spesa con quelle di acquisizione delle competenze adeguate per lo svolgimento dei compiti connessi alla migliore realizzazione degli obiettivi posti dalla disciplina europea a tutela dei diritti e delle libertà fondamentali degli interessati.

Infine, per quanto riguarda le descritte situazioni di affidamento a titolo gratuito in favore di società consortili che forniscono altri servizi (soprattutto in campo IT), si fa presente che la questione del compenso (in questo caso non previsto) rappresenta una conseguenza di un'altra problematica posta a monte, e cioè quella del conflitto di interessi in capo alla società (ampiamente trattata al par. 10.2). Un'applicazione rigorosa del principio di separazione tra servizi forniti da un soggetto in qualità di responsabile del trattamento, ai sensi dell'art. 28 del Regolamento, e i servizi forniti da un soggetto esterno in qualità di RPD, ai sensi dell'art. 37 del Regolamento, dovrebbe naturalmente condurre all'incumulabilità dei due incarichi in capo allo stesso soggetto, risolvendo, pertanto, alla radice la questione della remunerazione.

7. Pubblicazione e comunicazione all'Autorità dei dati di contatto del RPD

Disposizione di riferimento del Regolamento. Art. 37, par. 7: *"Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo"*.

Riferimento nelle Linee guida del WP29: par. 2.6, pp. 16-17.

Precedenti decisioni del Garante. *"Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico"*, 15 dicembre 2017 (doc. web n. 7322110); provv. 12 marzo 2020, n. 56 (doc. web n. 9429218); provv. 1° ottobre 2020, n. 173 (doc. web n. 9483375); provv. 17 dicembre 2020, n. 272 (doc. web n. 9557593); provv. 11 febbraio 2021, n. 54 (doc. web n. 9556625).

Questioni emerse. Non sempre è risultato che i titolari del trattamento abbiano effettuato i due predetti adempimenti, vanificando così la necessaria trasparenza informativa nei confronti sia degli interessati (che in questo modo non sanno dell'esistenza di una figura cui rivolgere le proprie istanze in materia di trattamento dei propri dati personali) che dell'Autorità medesima (facendo venire meno quel punto di contatto essenziale per lo svolgimento dei propri compiti istituzionali).

Inoltre, in alcuni casi l'ente ha ritenuto di poter assolvere all'obbligo di pubblicazione mediante l'affissione dei dati di contatto presso i propri uffici, senza la messa a disposizione su pagine facilmente individuabili all'interno del proprio sito web istituzionale.

Per quanto concerne, invece, l'adempimento della comunicazione dei dati di contatto all'Autorità, oltre ai numerosi casi di mancato assolvimento, si sono registrati anche altrettanto numerose situazioni di comunicazione effettuata mediante canali inadeguati (non avvalendosi cioè dell'apposita procedura *online* messa a disposizione dal Garante), oppure indicando riferimenti non corretti dell'ente titolare del trattamento (ad esempio, indicando il legale rappresentante come titolare del trattamento o fornendo, in luogo del codice fiscale dell'ente, la partita IVA, ovvero il codice fiscale del proprio legale rappresentante oppure del RPD medesimo), impedendone così l'individuazione.

Misure indicate. Ciascun soggetto che designa un RPD è tenuto ad effettuare entrambi gli adempimenti previsti dall'art. 37, par. 7, del Regolamento (pubblicazione e comunicazione all'Autorità dei dati di contatto).

Per quanto concerne la pubblicazione, questa dovrà essere effettuata sul sito web dell'amministrazione, all'interno di una sezione facilmente riconoscibile dall'utente e accessibile già dalla *homepage*, oltre che nell'ambito della sezione dedicata all'organigramma dell'ente ed ai relativi contatti.

Non è necessario che, tra i dati oggetto di pubblicazione, vi sia anche il nominativo del RPD, non essendo questa informazione indispensabile a fini di contatto da parte di chiunque sia

interessato: al contrario, risulta imprescindibile che tra i dati di contatto vi sia quantomeno un indirizzo di posta elettronica (sicuramente ordinaria, eventualmente integrata con un indirizzo PEC).

A proposito dell'indirizzo di posta elettronica, si invitano le amministrazioni a rendere disponibili, sia nei confronti del pubblico che dell'Autorità, una casella "istituzionale" *ad hoc* attribuita specificamente al solo RPD, evitando l'utilizzo di caselle che siano direttamente espressione del titolare del trattamento (ad esempio, perché richiamano l'"amministrazione", la "segreteria" o il "protocollo"). Invero, perché sia effettivamente indipendente nell'esercizio delle sue funzioni (come richiesto dal cons. 97 del Regolamento), sarebbe opportuno che il RPD venisse contattato attraverso canali che riconducano direttamente a lui, senza l'intermediazione di uffici facenti capo al titolare.

Per quanto concerne la comunicazione all'Autorità, si evidenzia che il Garante ha reso disponibile un'apposita procedura *online* non solo per la comunicazione, ma anche per la variazione e la revoca del nominativo del RPD designato. Tale procedura rappresenta l'unico canale di contatto utilizzabile a questo specifico fine ed è reperibile alla pagina <https://servizi.gpdp.it/comunicazionerpd/s/>, ove sono riportate anche le apposite istruzioni e le relative FAQ: peraltro, si richiama l'attenzione degli enti a inserire correttamente i dati richiesti, come l'individuazione del titolare del trattamento (l'ente complessivamente inteso, e non il legale rappresentante) e la compilazione del codice fiscale dell'amministrazione (e non della partita IVA, ovvero del codice fiscale di altro soggetto).

Per quanto concerne la variazione dei dati di contatto del RPD (ad esempio, per effetto della nomina di un differente soggetto per quell'incarico), essa dovrà essere effettuata tempestivamente, in modo che l'Autorità, per l'esercizio dei propri compiti, sia sempre in possesso di informazioni aggiornate e, conseguentemente, si rivolga al "punto di contatto" esatto.

Infatti, il mantenimento di dati di contatto non più attuali potrebbe comportare il coinvolgimento di un soggetto cessato dalle proprie funzioni di RPD, con conseguente comunicazione a terzi di informazioni che non ha più alcun titolo a conoscere: ad esempio, da parte di un interessato che si vuole rivolgere a lui ai sensi dell'art. 38, par. 4, del Regolamento, ovvero da parte della stessa Autorità, che lo intende coinvolgere nell'ambito di un procedimento, ai sensi dell'art. 39, par. 1, lett. d), ed e), del Regolamento.

Occorre considerare al riguardo che il mancato aggiornamento dei dati di contatto del RPD, tanto sul sito *web* dell'ente quanto nella relativa comunicazione all'Autorità, costituisce una condotta sanzionabile al pari della mancata pubblicazione/comunicazione.

8. Coinvolgimento da parte del titolare e svolgimento dei compiti da parte del RPD

Disposizioni di riferimento del Regolamento. Art. 38, par. 1: *"Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali"*.

Art. 38, par. 3: *"Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento"*.

Art. 39, par. 1: *"Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; d) cooperare con l'autorità di controllo; e e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione."*

Riferimento nelle Linee guida del WP29: par. 3.1, pp. 17-18; par. 4, pp. 22-25.

Precedenti decisioni del Garante. Relazione annuale 2019, par. 4.9 (pp. 80-81); provv. 17 dicembre 2020, n. 280 (doc. web n. 9524175); provv. 25 febbraio 2021, n. 87 (doc. web n. 9556958).

Questioni emerse. In alcuni dei casi in cui il RPD è una persona giuridica che fornisce tale servizio ad una pluralità di enti pubblici, è emerso che le interlocuzioni con i titolari non fossero sufficientemente frequenti.

In particolari situazioni, sono stati altresì lamentati, da parte di alcuni enti pubblici, veri e propri inadempimenti da parte del RPD designato, il quale non avrebbe svolto, in maniera adeguata, i compiti previsti dall'art. 39 del Regolamento, o quelli pattuiti all'atto del conferimento dell'incarico (quali, ad esempio, l'attività formativa nei confronti dei dipendenti, oppure il coordinamento nella mappatura dei trattamenti) e il conseguente supporto nello

svolgimento degli adempimenti previsti dalla disciplina in materia di protezione dei dati personali.

Anche nel caso di RPD interni si sono registrate situazioni di scarso coinvolgimento, da parte del titolare, soprattutto in occasione delle interlocuzioni avviate con l'Autorità nel corso di specifici procedimenti, con l'effetto di rendere difficoltosa l'acquisizione degli elementi necessari per chiarire i contorni dei trattamenti indagati.

Si osserva, in proposito, che la prassi di instaurare contatti, solo saltuari, tra il soggetto pubblico e il proprio RPD (sia interno che esterno) vanifica il senso della presenza del RPD e, con esso, l'approccio di *privacy by design* e *by default* promosso dal Regolamento, con conseguenze dirette in capo agli enti stessi in termini di *accountability* e di inadempimento agli obblighi regolamentari (ad esempio, ai sensi degli art. 82 e 83 del Regolamento).

In base alle risultanze fornite dall'attività ispettiva espletata dall'Autorità, ma anche dalle segnalazioni ricevute, si è riscontrato che tale atteggiamento può essere imputabile a entrambe le parti: al RPD, in quanto spesso portato a non proporre adeguatamente al titolare le attività necessarie per conformare i trattamenti alla disciplina in materia di protezione dei dati personali; all'ente pubblico, per la tendenza a considerare la nomina del RPD solo come un adempimento formale, non riconoscendo e tantomeno valorizzando i compiti e le potenzialità di questa figura.

Misure indicate. Nel corso delle indagini sul campo svolte dall'Autorità, sono, in ogni caso, emerse delle buone pratiche che si ritiene utile suggerire, in aggiunta a quelle già indicate nelle Linee guida del WP29, al fine di rendere effettivo il coinvolgimento del RPD e appropriato lo svolgimento dei compiti da parte di quest'ultimo:

- a) l'individuazione, all'interno dell'amministrazione, di una figura, adeguata per posizione e competenze, che funga da punto di riferimento per il RPD, con il quale quest'ultimo possa interloquire costantemente, al fine di ricevere gli elementi richiesti per lo svolgimento dei propri compiti, oltre che facilitare il dialogo con il vertice amministrativo;
- b) la condivisione di un'agenda attraverso la quale fissare momenti di dialogo con una congrua periodicità;
- c) la proposta, da parte del RPD al titolare, di attività da svolgere per migliorare la gestione dei trattamenti sul piano della conformità alla disciplina di settore, da effettuarsi sia al momento dell'assunzione dell'incarico che, periodicamente, in corso di esecuzione dello stesso. Tra queste, potrebbe, ad esempio, rientrare la predisposizione di:
 - c.1) documenti informativi, rivolti tanto al vertice dell'ente quanto ai suoi dipendenti e collaboratori;
 - c.2) attività di supporto per l'adempimento di singoli obblighi previsti dal Regolamento quali: le informative (artt. 12-14); le designazioni dei responsabili del trattamento (art. 28) e delle persone autorizzate (art. 29), con suggerimenti circa le possibili istruzioni da impartire; il registro dei trattamenti (art. 30); il registro delle violazioni (art. 33);

- c.3) proposte di misure tecniche e organizzative per innalzare il livello generale di protezione dei dati personali, oggetto dei trattamenti effettuati e per una più efficace tutela dei diritti e delle libertà fondamentali degli interessati;
- c.4) procedure interne per la gestione di eventi particolari quali le violazioni di dati personali di cui agli artt. 33 e 34 del Regolamento, o le valutazioni di impatto sulla protezione dei dati di cui all'art. 35 del Regolamento, o anche, più in genere, l'analisi dei rischi;
- d) la rendicontazione dell'attività svolta, sia quella *in loco* (mediante, ad esempio, la stesura di verbali degli incontri), sia quella a distanza;
- e) lo svolgimento di attività di formazione e aggiornamento rivolte alle persone autorizzate al trattamento dei dati dall'ente, da effettuarsi anche mediante la messa a disposizione di idonea documentazione.

Al fine di vincolare maggiormente i RPD allo svolgimento dei compiti che spettano loro, in particolare quando si tratta di soggetti esterni, si suggerisce agli enti pubblici di specificare espressamente tali attività tra gli obblighi contrattuali, pur nel rispetto del divieto di rimozioni o penalizzazioni per l'adempimento dei propri compiti di cui all'art. 38, par. 3, del Regolamento.

Non devono essere invece assegnati al RPD compiti che spettano al titolare del trattamento e che esulano dalle attività di consulenza, sorveglianza e, più in generale, consultazione, stabilite dall'art. 39 del Regolamento – nonché, eventualmente, di tenuta del registro delle attività di trattamento di cui all'art. 30 del Regolamento (cfr. le Linee guida del WP29, par. 4.5, pp. 24-25). Pur riconoscendo che i compiti ivi elencati costituiscono solo una rappresentazione esemplificativa, rimane comunque il fatto che il RPD non possa essere chiamato a svolgere, in prima persona, attività che, in base al Regolamento, competono al titolare/responsabile, peraltro a pena di applicazione di una sanzione amministrativa in caso di violazione. A questo proposito, infatti, milita anche il par. 3 dell'art. 38 del Regolamento, laddove vieta la rimozione o la penalizzazione del RPD per l'adempimento dei propri compiti, confermando, pertanto, che il suo ruolo è di supporto al titolare/responsabile, anche di controllo, ma non può da questo essere delegato rispetto a compiti esecutivi (e connesse responsabilità) che, nell'ottica del principio di *accountability*, spettano proprio al titolare (o al responsabile).

Potrebbe rivelarsi molto utile che i RPD che operano in un medesimo settore, o che condividano medesime problematiche, istituiscano tavoli di lavoro comuni e, in particolare, "reti di RPD", ove possano essere individuate soluzioni condivise anche attraverso l'analisi di problematiche comuni.

In questo senso, sono da incoraggiare iniziative già avviate come, ad esempio, le reti di RPD istituite nei settori della ricerca pubblica, della fiscalità o della sanità, ma anche a livello di Ministeri, Autorità indipendenti o su base regionale. Analoghe iniziative potrebbero essere promosse in tanti altri campi, al fine ultimo di favorire la sensibilizzazione dei titolari/responsabili sulle questioni di protezione dei dati personali, in un contesto di sempre maggiore sviluppo verso la digitalizzazione della pubblica amministrazione e dei suoi servizi.

9. Risorse messe a disposizione dal titolare e costituzione di un gruppo di collaboratori (team) del RPD

Disposizione di riferimento del Regolamento. Art. 38, par. 2: *"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"*.

Riferimento nelle Linee guida del WP29: par. 3.2, pp. 18-19.

Precedenti decisioni del Garante. *"Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico"*, 15 dicembre 2017 (doc. web n. 7322110); Relazione annuale 2019, par. 4.9 (pp. 80-81).

Questione emersa. Soprattutto nelle grandi amministrazioni i trattamenti effettuati possono essere numerosi, complessi e coinvolgere un'elevata quantità di dati personali, anche delicati: si pensi ai Ministeri o alle altre amministrazioni centrali, oppure alle Regioni o ai Comuni capoluogo. Inoltre, alcuni di questi enti sono dotati di una potestà normativa di rango primario e/o secondario, cui si aggiunge, in alcuni casi anche l'adozione di atti amministrativi di carattere generale, attraverso i quali possono concorrere a disciplinare trattamenti di dati personali.

In questi contesti aumenta significativamente il livello di difficoltà nell'esercizio dei compiti richiesti al RPD, sia per quanto concerne il possesso di un livello piuttosto diversificato e approfondito di conoscenze specialistiche, che per quanto concerne il tempo e le energie da dedicare alle tante istanze che emergono in materia di protezione dati. Ciò significa che la persona individuata quale RPD, da sola, difficilmente può essere in grado di assolvere ai propri compiti in maniera efficace e qualitativamente adeguata.

Misure indicate. Come già richiamato nelle Linee guida del WP29 e nelle precedenti FAQ del Garante, in rapporto alle dimensioni e alla complessità dei trattamenti effettuati, occorre valutare attentamente l'opportunità/necessità di istituire un apposito gruppo di persone (*team*) a supporto del RPD, al quale destinare le risorse necessarie allo svolgimento dei compiti stabiliti. A questo fine, un valore aggiunto potrebbe essere dato dalla scelta di destinare, a questo *team*, personale in possesso di competenze diversificate come, ad esempio, soggetti dal profilo più strettamente giuridico e amministrativo, e soggetti esperti in ambito IT.

Inoltre, anche in aggiunta alla costituzione del *team* di collaboratori, in amministrazioni grandi, potrebbe risultare anche opportuno individuare specifici referenti del RPD all'interno delle varie articolazioni dell'ente, 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. Incompatibilità con altri incarichi e conflitto di interessi

Disposizioni di riferimento del Regolamento. Art. 38, par. 3: *"Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento".*

Art. 38, par. 6: *"Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi".*

Cons. 97: *"[...] Tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente".*

Riferimento nelle Linee guida del WP29: par. 3.3, pp. 19-20; par. 3.5, pp. 21-22.

Questioni emerse. L'Autorità ha riscontrato numerose situazioni in cui viene nominato, quale RPD, un soggetto che svolge altri compiti che possono determinare un'incompatibilità o una situazione di conflitto di interessi, in quanto tali ulteriori incarichi gli impediscono di svolgere la propria attività di RPD con la necessaria indipendenza.

Ciò si può verificare allorché la figura individuata quale RPD rivesta, all'interno dell'organizzazione dell'ente, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali (ad esempio, perché contribuisce a definire le caratteristiche del trattamento *by design* e *by default*, oppure perché le sono attribuiti potestà decisionali all'esito di trattamenti di dati personali di particolare delicatezza). Parimenti, le medesime problematiche si riscontrano, con riferimento al RPD di provenienza esterna, qualora quest'ultimo sia assoggettato alle istruzioni impartite dal titolare del trattamento (ad esempio, perché sia stato da quest'ultimo designato quale responsabile del trattamento ai sensi dell'art. 28 del Regolamento per la fornitura di un determinato servizio, ovvero perché lo rappresenti in giudizio su problematiche in materia di protezione dei dati personali).

In proposito, le Linee guida del WP29 raccomandano buone pratiche, quali quelle di individuare preventivamente le qualifiche e funzioni che sarebbero incompatibili con quella di RPD e redigere regole interne onde evitare conflitti di interessi. Tuttavia, all'atto pratico, non è stata riscontrata una diffusa sensibilità sull'argomento.

Per queste ragioni, anche dopo aver raccolto gli orientamenti adottati dalle Autorità degli altri Stati membri, e fatte salve le indicazioni già fornite nelle citate Linee guida, si propone di seguito una specifica declinazione delle problematiche rilevate, con alcune proposte volte ad assicurare il rispetto delle intenzioni manifestate dal legislatore europeo.

- 10.1. RPD interno che ricopre incarichi per i quali partecipa all'adozione delle decisioni in materia di finalità e modalità del trattamento, o altre decisioni che impattano su trattamenti di dati personali

Precedenti decisioni del Garante. *"Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico"*, 15 dicembre 2017 (doc. web n. 7322110); Relazione annuale 2019, par. 4.9 (p. 81);

Questioni emerse. Il tema dell'incompatibilità con altri incarichi, e quindi della creazione di una situazione di conflitto di interessi, con riferimento a un RPD interno, è emersa in numerosi casi, in cui il soggetto individuato quale RPD, al contempo, rivestiva incarichi quali quello di componente di un organismo collegiale (ad esempio, un comitato direttivo o un collegio disciplinare) o di titolare di un incarico monocratico dotato di poteri decisionali (ad esempio, vicepresidente, dirigente degli affari generali, direttore amministrativo).

Più in generale, il tema si pone spesso in relazione alla scelta, da parte di soggetti pubblici dalle dimensioni e funzioni più diversificate, di affidare il ruolo di RPD a figure già deputate ad assolvere altri specifici incarichi che comportano poteri decisionali in ordine a finalità e mezzi dei trattamenti posti in essere: si pensi, *in primis*, a quelli in materia di trasparenza e/o di prevenzione della corruzione.

In particolare, altre situazioni di conflitti di interessi si possono registrare con riferimento alla sovrapposizione dell'incarico di RPD con quello di dirigente dell'unità organizzativa chiamata a curare la valutazione d'impatto sulla protezione dei dati relativa ad uno specifico trattamento, considerato che, a questo proposito, al RPD spettano specifiche prerogative di consultazione, da parte del titolare del trattamento (artt. 35, par. 2, e 39, par. 1, lett. c), del Regolamento), che verrebbero del tutto svuotate per effetto della citata coincidenza soggettiva.

Misure indicate. Nelle Linee guida del WP29 e nelle FAQ del Garante sono state già indicate situazioni di conflitto di interessi in relazione a ruoli manageriali di vertice come quelli, tra gli altri, di "[...] *responsabile finanziario* [...] *direzione risorse umane, responsabile IT*", di "*responsabile per la prevenzione della corruzione e per la trasparenza*" o di "*responsabile dei Sistemi informativi* [...] *ovvero quello dell'Ufficio di statistica*". In ogni caso, le medesime Linee guida specificano che l'indagine va fatta "*caso per caso guardando alla specifica struttura organizzativa del singolo titolare del trattamento o responsabile del trattamento*": ciò significa che solo l'esame concreto di ciascuna singola realtà – considerando elementi quali le dimensioni dell'ente, le risorse a disposizione, la complessità della struttura, le tipologie di trattamenti svolti, qualità e quantità dei dati trattati, ecc. – potrà condurre ad una valutazione definitiva sulla sussistenza o meno di cause di incompatibilità. Tale valutazione, in ogni caso, dovrà essere fornita dal titolare del trattamento, anche sulla base di idonea documentazione, in virtù del principio di *accountability* di cui agli artt. 5, par. 2, e 24 del Regolamento.

Ciò detto, per quanto concerne incarichi di carattere monocratico (quali quelli di dirigente direttamente coinvolto da trattamenti, o addirittura di vertice dell'ente), il conflitto di interessi,

spesso, diviene evidente *icto oculi*, e difficilmente si rende possibile comprovare, da parte del titolare del trattamento, che il medesimo soggetto che determina i trattamenti rientranti nel proprio settore abbia la necessaria indipendenza per esercitare, in maniera corretta, trasparente ed imparziale, quei compiti di sorveglianza sull'osservanza della disciplina e sulle politiche del titolare in materia di protezione dei dati personali, previsti dall'art. 39, par. 1, lett. b), del Regolamento. Si può certamente affermare la sussistenza di un conflitto di interessi in relazione ai ruoli già citati (come la direzione risorse umane o contabilità, il responsabile IT o il responsabile della prevenzione della corruzione e della trasparenza), trattandosi di settori in cui i trattamenti dei dati personali sono certi e trasversali rispetto all'intera amministrazione, oltre che significativi in termini di quantità e qualità dei dati personali trattati, nonché di rischi sui diritti e sulle libertà fondamentali degli interessati. Peraltro, altre Autorità europee si sono già pronunciate espressamente in proposito (invero con riferimento all'ambito privato), sancendo l'incompatibilità tra la figura di RPD e quella di responsabile IT (provv. dell'Autorità bavarese del 20 ottobre 2016) o quella di dirigente dei dipartimenti che si occupano di conformità normativa, della gestione del rischio e di *audit* interni (provv. dell'Autorità belga n. 18/2020 del 28 aprile 2020).

Tutto ciò considerato, si ritiene che tali tipologie di incarichi siano incompatibili con quello di RPD, quantomeno per quanto riguarda le grandi amministrazioni che dispongono delle risorse tali per potersi avvalere di un RPD a ciò esclusivamente dedicato, o comunque che non versino in una situazione di potenziale conflitto di interessi. Ciò vale sia per gli enti pubblici di carattere nazionale (come Ministeri, Agenzie fiscali, grandi enti di ricerca ed altri grandi enti pubblici, ecc. che per quelli territoriali (Regioni, grandi strutture sanitarie, altri grandi enti di livello regionale, Comuni di rilevanti dimensioni, ecc.). Per quanto concerne gli enti che, sul piano delle dimensioni, delle risorse e dell'organizzazione, presentano difficoltà oggettive ad avvalersi di una figura esclusivamente dedicata a ricoprire l'incarico di RPD, il titolare dovrà effettuare una ponderazione *ad hoc*, mettendo a disposizione dell'Autorità (laddove necessario) le valutazioni all'uopo effettuate ai sensi degli artt. 5, par. 2, e 24 del Regolamento, al fine di valutare il rischio effettivo di conflitto di interessi nell'ambito e nel contesto dei trattamenti svolti dall'amministrazione.

Discorso diverso, invece, vale per quei soggetti che partecipano a organismi collegiali, ancorché di vertice. Infatti, in questi casi, è possibile che la normativa vigente contempli misure che possono ritenersi adeguate a prevenire rischi di conflitti di interessi, come, ad esempio, la previsione che i componenti che ritengano di trovarsi in tale situazione, lo dichiarino e, conseguentemente, si astengano sia dalla discussione che dalla deliberazione. Per queste ragioni, si ritiene che il componente di tale organismo collegiale, qualora investito dell'incarico di RPD, non versino, per ciò stesso, in una situazione di conflitto di interessi, a condizione che siano presenti e pienamente rispettate misure di prevenzione dei conflitti di interessi.

In ogni caso, l'ente deve tenere nella dovuta considerazione il fatto che l'accumulo di incarichi ulteriori sulla figura chiamata a svolgere il ruolo di RPD inficia la capacità del medesimo di assolvere efficacemente ai compiti assegnatigli dal Regolamento. L'amministrazione, pertanto, dovrebbe valutare, in relazione alla complessità della struttura organizzativa, alla disponibilità di risorse, alla numerosità e delicatezza dei trattamenti svolti, alla quantità e

qualità di dati personali trattati, di affidare l'incarico di RPD a una persona che possa dedicarvisi tendenzialmente a tempo pieno.

10.2. RPD esterno che fornisce servizi IT quale responsabile del trattamento

Questione emersa. Nel corso dell'attività svolta dall'Autorità sono emersi numerosi casi in cui soggetti che forniscono servizi (prevalentemente del settore IT) a pubbliche amministrazioni, in qualità di responsabili del trattamento ai sensi dell'art. 28 del Regolamento, forniscono, al contempo, il servizio di RPD, beneficiando del preesistente legame instaurato con il titolare del trattamento.

Tali persone giuridiche indicano una persona fisica del proprio organigramma che funga da referente, e, talora, gli forniscono un *team* di supporto: tuttavia, si sono registrate situazioni in cui il medesimo personale adibito al servizio di RPD, al contempo, svolgeva anche particolari compiti nell'ambito della prestazione principale offerta (ad esempio, assistenza tecnica sulle piattaforme messe a disposizione dell'ente).

Nella medesima situazione si ricade allorché venga designato, come RPD, non l'intera società, bensì una persona fisica che, per ruolo e poteri all'interno della predetta società, sia in grado di adottare decisioni che influiscano sulla fornitura dei servizi IT, e quindi impattino sui trattamenti di dati personali effettuati per conto dell'amministrazione titolare (ad esempio, l'amministratore delegato, il direttore amministrativo, o comunque chiunque rivesta un ruolo apicale al suo interno).

Questa sovrapposizione delle figure di RPD e di responsabile IT rende impossibile, di fatto, la sorveglianza, con la necessaria imparzialità, sulla validità e sull'adeguatezza delle soluzioni e delle misure, tecniche e organizzative, adottate, dato che i ruoli di controllore e controllato confluirebbero in capo al medesimo soggetto, ingenerando così un evidente conflitto permanente nello svolgimento delle proprie funzioni.

In altre parole, si ritiene che l'indipendenza che il cons. 97 del Regolamento richiede in capo al RPD, tradotta nel divieto di conflitti di interessi di cui all'art. 38, par. 6, si troverebbe ad essere minata, in questi casi, proprio in ragione delle istruzioni che, nel suo ruolo di responsabile del trattamento, lo stesso deve ricevere dal titolare, ai sensi dell'art. 28, par. 3, lett. a), andando così a compromettere anche il divieto di ricevere istruzioni di cui al par. 3 dell'art. 38.

L'attività di sorveglianza del RPD sarebbe pregiudicata, in particolare, in relazione alla valutazione delle caratteristiche richieste per l'avvalimento di fornitori esterni in qualità di responsabili del trattamento – su cui si esprime in maniera chiara l'art. 39, par. 1, lett. b), del Regolamento – proprio perché costui, in ragione del suo diretto coinvolgimento, non potrebbe giudicare, con la dovuta terzietà, i necessari requisiti di affidabilità, né potrebbe supportare adeguatamente il titolare nel processo di definizione del rapporto, ai sensi dell'art. 28 del Regolamento. A ciò si aggiunga l'ulteriore criticità, emersa in alcune specifiche ipotesi, in cui l'ente non abbia previamente stipulato, con il fornitore di servizi IT, l'accordo di cui all'art. 28 del Regolamento: un RPD effettivamente terzo avrebbe segnalato tale violazione e proposto soluzioni idonee a ripristinare la conformità.

Le ripercussioni di questa sovrapposizione diventano ancor più gravi in caso di violazioni di sicurezza, posto che i compiti del RPD potrebbero interferire, in maniera poco trasparente, con quanto previsto dagli artt. 33 e 34 del Regolamento, in termini di analisi dei rischi e delle conseguenze, di predisposizione delle misure da adottare per porvi rimedio e di comunicazione della violazione all'Autorità ed agli interessati. In ragione delle sue inevitabili implicazioni quale responsabile del trattamento, il RPD non avrebbe un ruolo terzo e di imparziale supporto al titolare nel giudicare le condotte sottese alla violazione di sicurezza.

Infine, questo conflitto di interessi si verifica in maniera ancor più eclatante allorché il fornitore IT fornisca all'amministrazione propri prodotti *software* (nonché la corrispondente assistenza tecnica) per l'implementazione dei servizi offerti. In questo modo, l'attività di consulenza del RPD, ai sensi dell'art. 39, par. 1, lett. a), del Regolamento, non assumerebbe i necessari caratteri dell'imparzialità, posto che il RPD si troverebbe a dover fornire giudizi su prodotti forniti dalla propria società.

Misure indicate. Alla luce delle tante criticità insite nella scelta di affidare il compito di RPD ad un soggetto che già fornisce servizi al medesimo ente – con particolare riferimento a quelli del settore IT – la principale soluzione consiste nel non designare, quale RPD, soggetti a cui l'amministrazione affida un trattamento per suo conto, con conseguente necessità di definizione di un rapporto titolare-responsabile.

In ogni caso, anche sulla scorta di esperienze mutate da altri Paesi europei, si propone una soluzione alternativa, subordinata però al rispetto di alcune condizioni.

In particolare, laddove l'ente, per specifiche ragioni, ritenga comunque di non poter prescindere dall'affidamento dell'incarico di RPD nel contesto di un fornitore di servizi, ciò potrebbe avvenire solamente a condizione che il RPD, o anche solo il suo referente persona fisica, non sia la persona che riveste una carica apicale nell'azienda, o anche solo nel settore di cui vengono forniti i predetti servizi. Inoltre, altra necessaria condizione da rispettare perché tale soluzione possa essere valutata, risiede nell'indispensabilità di una rigida separazione, all'interno dell'organizzazione societaria, tra attività rese come RPD e attività rese come responsabile del trattamento per altri servizi.

Nel caso in cui l'amministrazione intenda ricorrere a quest'ultima soluzione, considerato che le misure appena descritte, di per sé, non sono comunque sufficienti ad eliminare del tutto i rischi di conflitti di interessi, si renderà necessario comprovare adeguatamente il rispetto delle medesime, ai sensi degli artt. 5, par. 2, e 24 del Regolamento, documentando anche le ragioni ed il contesto in cui è maturata suddetta scelta.

In assenza di queste condizioni, si ritiene che il rischio di conflitto di interessi debba considerarsi elevato, e quindi che la scelta di affidare l'incarico di RPD al fornitore di servizi possa integrare una violazione del Regolamento.

Parimenti, si ritiene che il responsabile del trattamento non possa essere coinvolto nel processo di selezione del RPD da parte dell'ente, prerogativa che spetta unicamente al titolare, che la deve effettuare in autonomia. Ciò anche perché i rapporti tra titolare e responsabile sono oggetto di vigilanza da parte del RPD, ai sensi dell'art. 39, par. 1, lett. b), del Regolamento.

10.3. RPD esterno che rappresenta in giudizio il titolare

Questione emersa. Sono stati registrati anche casi in cui un Comune, a seguito di azione giudiziaria promossa da un cittadino, si sia costituito in giudizio per il tramite di un avvocato che, contemporaneamente, svolgeva l'incarico di RPD per conto del medesimo ente. Il Comune ha ritenuto che questa scelta non comportasse alcun conflitto di interessi in quanto il giudizio instaurato non verteva su profili di protezione dei dati personali.

Misura indicata. Come espressamente affermato dalle Linee guida, *"può insorgere un conflitto di interessi se, per esempio, a un RPD esterno si chiede di rappresentare il titolare o il responsabile in un giudizio che tocchi problematiche di protezione dei dati"*.

A questo proposito, si richiama l'attenzione degli enti pubblici sul fatto che è difficile prevedere a priori che una vertenza giudiziaria non possa coinvolgere anche profili di protezione dei dati personali. A ciò si aggiunga che, in ogni caso, agli occhi dell'interessato che voglia rivolgersi al RPD, la circostanza che questo sia contemporaneamente anche il difensore in giudizio dell'ente, mina la sua indipendenza.

Pertanto, a prescindere dalle circostanze che in concreto si potranno realizzare – tali, ad esempio, da escludere che il giudizio involva questioni di protezione dei dati personali – si invitano tutte le pubbliche amministrazioni a designare un RPD che, contemporaneamente, non svolga per le medesime il ruolo di difensore in giudizio.

10.4. Inquadramento in caso di RPD interno

Precedente decisione del Garante. *"Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico"*, 15 dicembre 2017 (doc. web n. 7322110).

Questione emersa. È opportuno 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 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 caso di RPD interno, qualora il soggetto designato abbia una qualifica tale da renderlo sottoposto ad un'altra figura (come un funzionario inquadrato in un'unità organizzativa, e quindi subordinato ad un dirigente), tale rapporto potrebbe impedire al RPD di svolgere le proprie mansioni con il dovuto grado di autonomia, e potrebbe altresì alterare la diretta interlocuzione con il vertice gerarchico dell'ente.

Misura indicata. L'art. 38 del Regolamento fissa alcune garanzie essenziali per consentire ai RPD di operare con un grado sufficiente di autonomia all'interno dell'organizzazione, mentre il rapporto diretto con il vertice amministrativo garantisce, in particolare, che quest'ultimo venga a conoscenza delle indicazioni e delle raccomandazioni

fornite dal RPD nell'esercizio delle funzioni di informazione e consulenza a favore del titolare/responsabile.

Pertanto, 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.

In caso di individuazione di un funzionario, occorre però che l'ente adotti delle idonee garanzie affinché l'attività svolta in qualità di RPD non subisca interferenze per effetto dell'inquadramento del medesimo soggetto in un'unità organizzativa retta da un dirigente le cui determinazioni potrebbero essere oggetto di valutazione da parte del RPD.