LO STATUTO DEL RESPONSABILE DELLA PROTEZIONE DEI DATI

Orientamenti sul quadro di esercizio delle funzioni, sull'indipendenza, sulle garanzie organizzative e sui conflitti di interessi

Agenzia spagnola per la protezione dei dati (AEPD)

Guida pubblicata nel novembre 2026.

Traduzione italiana integrale non ufficiale dell'originale in lingua spagnola. Ai fini dell'interpretazione e dell'applicazione del diritto spagnolo fa fede il testo originale dell'AEPD. I richiami alla Ley Orgánica 3/2018 (LOPDGDD) e alla giurisprudenza nazionale spagnola restano riferiti all'ordinamento spagnolo; non costituiscono indicazioni circa l'applicabilità di tali disposizioni in Italia.

Indice

I numeri di pagina riportati nell'indice si riferiscono al documento originale spagnolo.

Presentazione — pagina 5 dell'originale

I. Sintesi esecutiva — 9

II. Designazione del RPD — 10

A. Qualifiche professionali del RPD — 10

B. Procedura di designazione del RPD — 11

III. Indipendenza quale garanzia di efficacia — 19

A. Indipendenza funzionale — 20

B. Indipendenza gerarchica — 20

C. Conflitti di interessi — 20

D. Indipendenza economica — 21

E. Indipendenza organizzativa — 22

IV. Reporting e rendicontazione del RPD — 23

Il reporting del RPD quale strumento di governance e responsabilizzazione — 23

A. Meccanismi di reporting proporzionati alle dimensioni e alla complessità dell'organizzazione — 24

B. Comunicazione diretta con l'alta direzione — 25

C. Documentazione della consulenza e tracciabilità delle decisioni — 25

D. Comunicazione di rischi, incidenti e violazioni rilevanti — 26

E. Relazioni periodiche sull'attività quale buona prassi avanzata — 26

Risorse organizzative necessarie per un reporting efficace — 27

V. Garanzie organizzative relative alla nomina, alla permanenza nell'incarico e alla cessazione — 27

A. Designazione formale del RPD quale garanzia di indipendenza istituzionale — 27

B. Partecipazione del RPD alle decisioni che incidono sulla sua posizione istituzionale — 28

C. Indipendenza del RPD quale principio informatore del suo statuto giuridico — 29

D. Tutela contro la rimozione dall'incarico e le misure sanzionatorie — 30

E. Garanzie rafforzate di permanenza nell'incarico — 30

F. Motivazione delle decisioni che incidono sul RPD — 31

G. Tutela contro le misure organizzative che incidono sostanzialmente sull'indipendenza del RPD — 31

H. Tutela contro le ritorsioni e garanzie organizzative minime — 32

VI. Il RPD e la vigilanza sul principio di responsabilizzazione — 33

A. Politiche di protezione dei dati — 34

B. Predisposizione e aggiornamento del registro delle attività di trattamento (RAT) e dell'inventario delle attività di trattamento — 35

C. Valutazione d'impatto sulla protezione dei dati (DPIA) — 37

D. Violazioni della sicurezza dei dati personali — 38

E. Audit in materia di protezione dei dati — 39

VII. Situazioni che richiedono una valutazione specifica dell'indipendenza del RPD — 40

A. Il RPD nelle procedure di affidamento — 41

B. RPD titolare di altri ruoli e responsabilità nell'organizzazione — 42

C. Posizioni organizzative potenzialmente compatibili — 45

D. Alcune situazioni che potrebbero compromettere l'indipendenza del RPD o favorire possibili conflitti di interessi — 47

VIII. Strumenti di tutela del RPD — 50

A. Consultazione o reclamo dinanzi all'autorità di controllo — 51

B. Tutela giurisdizionale — 51

IX. Conclusione — 51

X. Riferimenti — 55

A. Agenzia spagnola per la protezione dei dati — 55

B. Comitato europeo per la protezione dei dati e Garante europeo della protezione dei dati — 56

C. Autorità regionali — 57

D. Autorità di controllo di altri Stati — 57

E. Associazioni professionali, norme tecniche e altri riferimenti — 58

F. Giurisprudenza — 59

Presentazione

I responsabili della protezione dei dati svolgono una funzione essenziale per il rispetto della normativa sulla protezione dei dati personali e per la garanzia dei diritti degli interessati. Non lo affermiamo per mera cortesia. Lo affermiamo perché la protezione dei dati personali costituisce oggi una garanzia trasversale dei diritti delle persone nell'ambiente digitale e perché tale garanzia è effettiva soltanto quando, all'interno di ogni organizzazione, pubblica o privata, opera una figura dotata delle conoscenze, della posizione e dell'indipendenza necessarie per fornire consulenza con competenza e svolgere attività di vigilanza con obiettività. Per l'effettività di tale funzione è necessario che le organizzazioni, pubbliche e private, assicurino a coloro che la esercitano la posizione, le risorse — comprese quelle necessarie a mantenere aggiornate le conoscenze specialistiche — e l'indipendenza richieste per una consulenza e una vigilanza obiettive.

Questa funzione occupa una posizione centrale nel Piano strategico 2025–2030 dell'Agenzia spagnola per la protezione dei dati (AEPD). L'elaborazione del Piano si è basata su circa cinquanta incontri con associazioni professionali, imprese, pubbliche amministrazioni, università e organizzazioni della società civile, nonché su una consultazione pubblica che ha raccolto quasi cinquecento contributi, oltre un quinto dei quali provenienti da professionisti della privacy. Da tale processo è scaturito l'impegno a consolidare la posizione dei responsabili della protezione dei dati, rafforzarne l'indipendenza funzionale e la capacità di intervento e formulare proposte per chiarirne lo statuto giuridico, comprese le possibili incompatibilità con altre funzioni.

In tale contesto viene presentato «Lo statuto del responsabile della protezione dei dati. Orientamenti sul quadro di esercizio delle funzioni, sull'indipendenza, sulle garanzie organizzative e sui conflitti di interessi», frutto di un'elaborazione approfondita e pluralistica durata circa un anno. La bozza è stata sottoposta a due cicli di consultazione e confronto con associazioni professionali e persone che esercitano la funzione di RPD nel settore pubblico. Sono state inoltre raccolte le osservazioni del Consiglio per la trasparenza e la protezione dei dati dell'Andalusia e il testo è stato messo a disposizione dell'Autorità catalana per la protezione dei dati e dell'Autorità basca per la protezione dei dati, affinché lo esaminassero.

I contributi ricevuti hanno consentito di apportare modifiche sostanziali, confrontare gli orientamenti proposti con la pratica professionale e individuare le difficoltà e le esigenze connesse alla loro applicazione. Hanno così rafforzato il fondamento tecnico e l'utilità pratica del documento, che tiene conto della diversità delle organizzazioni e delle condizioni effettive di esercizio della professione.

Tale processo si inserisce nel principio di «Agenzia aperta» del Piano strategico 2025–2030 e contribuisce all'attuazione delle misure 4.1, 4.2, 4.3 e 7.3, riguardanti, rispettivamente: la cooperazione con i professionisti e le loro organizzazioni rappresentative; il rafforzamento dell'indipendenza e della capacità d'intervento dei responsabili della protezione dei dati e la chiarificazione del loro statuto giuridico; la collaborazione con le autorità regionali e altri organismi competenti; la consultazione e il confronto preliminari alla pubblicazione di guide e criteri. Quest'ultima misura rientra nell'asse 7 del Piano, «Apertura, prossimità e cultura della protezione dei dati».

Il presente documento affronta la designazione del responsabile della protezione dei dati; i criteri di indipendenza funzionale, gerarchica, economica e organizzativa; la rendicontazione nei confronti dell'alta direzione; le garanzie relative alla nomina, alla permanenza nell'incarico e alla cessazione; la vigilanza sul rispetto del principio di responsabilizzazione; la valutazione di possibili conflitti di interessi; gli strumenti di tutela disponibili.

Il suo scopo è fornire criteri interpretativi che agevolino l'applicazione delle garanzie previste dagli articoli da 37 a 39 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo

alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati, GDPR), e dagli articoli da 34 a 37 della legge organica spagnola 3/2018, del 5 dicembre, sulla protezione dei dati personali e la garanzia dei diritti digitali. Pertanto, il documento non introduce nuovi obblighi né impone un unico modello organizzativo.

Gli orientamenti si rivolgono tanto ai responsabili della protezione dei dati quanto ai titolari e ai responsabili del trattamento, nonché ai rispettivi organi direttivi. L'indipendenza nell'esercizio della funzione costituisce una garanzia istituzionale la cui effettività deve essere assicurata da ciascuna organizzazione.

Nell'elaborazione sono stati presi in considerazione il modello di istruzione interna sullo statuto del responsabile della protezione dei dati predisposto dal Consiglio per la trasparenza e la protezione dei dati dell'Andalusia, che ha costituito un precedente di particolare rilievo; i documenti di riferimento delle associazioni professionali; le relazioni e i provvedimenti dell'Agenzia spagnola per la protezione dei dati; la giurisprudenza della Corte di giustizia dell'Unione europea e dell'Audiencia Nacional.

Sono stati altresì esaminati i criteri e i documenti del Comitato europeo per la protezione dei dati e del Garante europeo della protezione dei dati, nonché quelli delle autorità di controllo di Francia — Commission nationale de l'informatique et des libertés —, Belgio — Autorité de protection des données / Gegevensbeschermingsautoriteit —, Italia — Garante per la protezione dei dati personali —, Paesi Bassi — Autoriteit Persoonsgegevens —, Irlanda — Data Protection Commission —, Finlandia — Tietosuojavaltuutetun toimisto —, Danimarca — Datatilsynet — e Svezia — Integritetsskyddsmyndigheten. Sono stati considerati anche riferimenti internazionali, come la norma ISO 37009:2025 sulla gestione dei conflitti di interessi.

Il testo potrà essere integrato alla luce dell'esperienza maturata nella sua applicazione. In particolare, è prevista l'elaborazione, in collaborazione con alcune delle associazioni professionali partecipanti, di buone prassi per prevenire e risolvere i conflitti di interessi in fattispecie concrete. A tal fine, l'Agenzia manterrà aperti i canali di raccolta delle osservazioni e delle proposte di miglioramento provenienti da chi applica gli orientamenti.

Questa iniziativa rientra in un più ampio insieme di attività di cooperazione con i professionisti della privacy. Nel corso del 2026, l'Agenzia ha intrattenuto un processo di dialogo e collaborazione con i responsabili della protezione dei dati dell'Amministrazione generale dello Stato, articolato in diversi incontri con professionisti del settore pubblico e privato e in un evento che ha riunito oltre settanta professionisti. Da tale processo sono scaturite raccomandazioni per rafforzare l'osservanza della normativa sulla protezione dei dati in tale ambito, nonché impegni e attività attualmente in corso di attuazione.

Tra le prossime linee di lavoro figura l'analisi del rapporto tra le funzioni di protezione dei dati e le responsabilità connesse all'intelligenza artificiale. L'emergere di nuovi ruoli organizzativi rende necessario delimitarne i rispettivi ambiti d'intervento, prevenire possibili conflitti di interessi e preservare l'indipendenza dei responsabili della protezione dei dati.

L'Agenzia spagnola per la protezione dei dati ringrazia per il tempo e l'esperienza messi a disposizione i componenti del Club del Delegado de Protección de Datos dell'Asociación Española para la Calidad (AEC), dell'Asociación Profesional Española de Privacidad e Inteligencia Artificial (APEP·IA), dell'Asociación de Expertos Nacionales de la Abogacía TIC (ENATIC) e dell'Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum), nonché i responsabili della protezione dei dati del settore pubblico che hanno partecipato al processo. Il ringraziamento si estende al personale dell'Agenzia e ai gruppi di lavoro che hanno contribuito alla predisposizione e alla revisione del documento.

Lorenzo Cotino Hueso
Presidente dell'Agenzia spagnola per la protezione dei dati

Francisco Pérez Bes
Aggiunto (*Adjunto*) dell'Agenzia spagnola per la protezione dei dati

I. Sintesi esecutiva

Il responsabile della protezione dei dati (RPD) rappresenta la figura centrale nel modello di conformità al regolamento generale sulla protezione dei dati (GDPR) e alla legge organica spagnola 3/2018 sulla protezione dei dati personali e la garanzia dei diritti digitali (LOPDGDD). Si tratta di normative fondate, fra l'altro, sul principio di responsabilizzazione (*accountability*), che impone ai titolari e ai responsabili del trattamento non solo di rispettare gli obblighi applicabili, ma anche di essere in grado di dimostrarne l'osservanza. I compiti principali del RPD sono disciplinati dall'articolo 39 del GDPR, cui si aggiungono quelli assegnati dall'articolo 37 della LOPDGDD, ferma restando la possibilità per il titolare o il responsabile del trattamento di affidargli ulteriori funzioni e competenze, purché non compromettano la sua indipendenza e non determinino conflitti di interessi.

Anche la reperibilità del RPD costituisce una caratteristica essenziale per il corretto esercizio delle sue competenze, poiché, nello svolgimento delle proprie funzioni, tale figura opera da collegamento fra il titolare o il responsabile del trattamento, l'autorità di controllo e gli interessati.

Per svolgere efficacemente i propri compiti, il RPD deve operare in modo indipendente: ciò significa che il titolare o il responsabile del trattamento devono garantire che il RPD da loro designato non riceva alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti. Non gli si può indicare come affrontare una questione relativa alla protezione dei dati, quali risultati debba raggiungere nelle proprie analisi, come debba esaminare una segnalazione o un reclamo, quale posizione debba assumere sull'opportunità di consultare l'autorità di controllo, né come debba interpretare la normativa. L'indipendenza deve dunque essere intesa in senso ampio, sia nei confronti dell'organizzazione di appartenenza sia nei confronti di altre organizzazioni.

Il Piano strategico 2025–2030 dell'AEPD rafforza e valorizza la figura del RPD sotto diversi profili essenziali, in linea con le sfide tecnologiche, la trasformazione digitale e l'esigenza di assicurare una conformità normativa solida e proattiva. In tale prospettiva si intende rafforzare la posizione e l'indipendenza del RPD, la sua integrazione nei processi decisionali delle organizzazioni e la sua formazione e qualificazione permanente, con attenzione sia alla pratica giuridica sia alle tecnologie emergenti. Si intende inoltre mettergli a disposizione strumenti adeguati e sufficienti e ulteriori risorse di supporto, per farne, in definitiva, il fulcro della cultura della protezione dei dati nelle organizzazioni pubbliche e private.

Consolidare la posizione dei RPD mediante elementi che ne rafforzino concretamente l'indipendenza, le conoscenze e le altre qualità necessarie all'efficace svolgimento della funzione costituisce una delle principali sfide. Lo ha sottolineato il Comitato europeo per la protezione dei dati (EDPB) nella relazione del gennaio 2024 sull'azione coordinata di applicazione della normativa relativa alla designazione e alla posizione dei RPD, che ha individuato, fra le criticità e le raccomandazioni, i conflitti di interessi e l'insufficiente indipendenza del RPD. La relazione osservava inoltre che le autorità di controllo possono adottare orientamenti che comprendano anche le nuove funzioni assunte dai RPD in forza dei nuovi atti legislativi dell'Unione europea in materia digitale.

La pubblicazione dei presenti orientamenti mira a favorire l'integrazione del RPD nelle organizzazioni e ad agevolarne l'attività nel quadro delle disposizioni del GDPR e della LOPDGDD che ne disciplinano l'operato, nonché delle normative settoriali che prevedono trattamenti di dati in ambiti specifici. Le indicazioni qui contenute sono dedicate principalmente alla garanzia dell'indipendenza del RPD nell'esercizio delle sue funzioni.

L’obiettivo ultimo di queste raccomandazioni è pertanto fornire al RPD e ai vertici delle organizzazioni che si avvalgono di tali servizi un quadro di certezza e sicurezza giuridica, a beneficio della tutela dei diritti e delle libertà delle persone fisiche.

II. Designazione del RPD

Il procedimento di designazione del RPD costituisce un elemento fondamentale per garantire la conformità al GDPR e alla legge organica spagnola 3/2018 sulla protezione dei dati personali e la garanzia dei diritti digitali (LOPDGDD). Di seguito vengono illustrate alcune considerazioni da valutare, in generale, prima della designazione e, in particolare, in ordine ai soggetti designabili, alle modalità del procedimento, ai requisiti legali e alle funzioni del RPD, nonché alle buone prassi raccomandate dall'EDPB.

A. Qualifiche professionali del RPD

L'articolo 37, paragrafo 5, del GDPR stabilisce che il RPD debba essere designato in funzione delle qualità professionali e, in particolare, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché della capacità di assolvere i compiti previsti dal GDPR. Nel contesto tecnologico attuale occorre tuttavia ricordare anche che il considerando 97[1] richiede che il livello necessario di conoscenze specialistiche sia determinato in funzione delle operazioni di trattamento effettuate e della protezione richiesta per i dati personali trattati dal titolare o dal responsabile. Nella pratica devono essere altresì considerate le competenze professionali maturate nell'ingegneria della privacy, nella riservatezza e nella protezione dei dati, nonché le conoscenze tecnologiche.

Con specifico riferimento ai trattamenti svolti dal titolare o dal responsabile, devono essere considerate le variabili relative al contesto, alla natura, alle finalità e all'ambito o alla portata di tali trattamenti. Ciò comporta, nella pratica, competenze giuridiche (GDPR, LOPDGDD, normative settoriali ecc.), competenze tecniche (tecnologie emergenti, protezione dei dati fin dalla progettazione e per impostazione predefinita, misure di sicurezza, gestione dei rischi ecc.) e competenze organizzative (capacità di gestione dei processi interni, conoscenza dell'organizzazione, buone prassi di governance ecc.), aspetti evidenziati anche nelle linee guida dell'EDPB[2].

L'inserimento di tale figura nell'organizzazione può avvenire secondo diverse modalità: un dipendente interno (per esempio, un avvocato, un responsabile della compliance o un esperto IT); un professionista esterno (per esempio, un consulente, un avvocato specializzato o una società che presta servizi di protezione dei dati); un gruppo di persone (nelle organizzazioni di grandi dimensioni può esservi un team privacy coordinato dal RPD); oppure un RPD affidato contrattualmente all'esterno a tempo pieno o parziale (in tal caso, l'impresa affidataria designa una persona fisica come RPD dell'organizzazione cliente).

Oltre alle conoscenze specialistiche in materia giuridica e di prassi sulla protezione dei dati, alla conoscenza dell'organizzazione e dei suoi processi e delle caratteristiche tecnologiche dei trattamenti, occorre considerare le cosiddette competenze trasversali (*soft skills*), ossia quelle capacità relazionali necessarie per interagire con tutte le componenti organizzative esercitando il pensiero critico richiesto al RPD. Fra queste possono rientrare le capacità di comunicazione e lavoro di squadra, l'adattabilità ai cambiamenti e agli imprevisti, l'empatia, l'intelligenza emotiva, la gestione del tempo e l'attitudine alla risoluzione dei conflitti.

Nota 1. Il livello di conoscenze specialistiche richiesto deve essere determinato, in particolare, in funzione delle operazioni di trattamento effettuate e della protezione richiesta per i dati personali trattati dal titolare o dal responsabile del trattamento.

Nota 2. WP243: la capacità del RPD di assolvere i propri compiti deve essere interpretata alla luce sia delle qualità personali e delle conoscenze, sia della sua posizione all'interno dell'organizzazione. Le qualità personali devono includere, per esempio, l'integrità e un elevato livello di etica professionale; la principale preoccupazione del RPD deve essere quella di consentire il rispetto del GDPR. Il RPD riveste un ruolo fondamentale nella promozione della cultura della protezione dei dati nell'organizzazione e contribuisce all'attuazione di elementi essenziali del GDPR,

quali i principi relativi al trattamento, i diritti degli interessati, la protezione dei dati fin dalla progettazione e per impostazione predefinita, il registro delle attività di trattamento, la sicurezza del trattamento e la notificazione e comunicazione delle violazioni dei dati personali.

B. Procedura di designazione del RPD

La designazione del RPD può avvenire mediante l'istituzione di un organo collegiale oppure attraverso l'individuazione di una determinata persona. La soluzione collegiale consente di adeguare la funzione alle caratteristiche di un organismo pubblico o di un soggetto privato. Per esempio, un raggruppamento temporaneo di imprese (UTE, secondo la terminologia spagnola) può istituire un ufficio per la protezione dei dati che eserciti le funzioni del RPD per l'intero raggruppamento, avvalendosi di persone appartenenti a ciascuna delle entità che lo compongono e, contestualmente, di una consulenza esterna contrattualizzata. I vantaggi dell'organo collegiale sono evidenti: l'esercizio delle funzioni del RPD non dipende dalla presenza fisica di un'unica persona e, in caso di conflitto di interessi, possono essere adottati meccanismi di astensione che non pregiudicano il regolare svolgimento dei compiti del RPD né ostacolano le attività dei titolari o dei responsabili del trattamento.

Indipendentemente dal fatto che la designazione riguardi un organo collegiale o una persona fisica, il procedimento deve essere formale, documentato e trasparente e può articolarsi nelle fasi seguenti.

1. Individuare la necessità o l'obbligo di designare un RPD

Prima della designazione, l'organizzazione deve verificare se vi sia tenuta ai sensi dell'articolo 37 del GDPR e dell'articolo 34 della LOPDGDD. Le situazioni che impongono la designazione obbligatoria sono:

- autorità e organismi pubblici (eccettuate le autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali);
- trattamenti su larga scala di categorie particolari di dati personali (salute, opinioni politiche, appartenenza sindacale ecc.);
- trattamenti su larga scala di dati relativi a condanne penali e reati;
- monitoraggio regolare e sistematico degli interessati su larga scala (per esempio, videosorveglianza, profilazione degli utenti dei social network);
- soggetti specificamente indicati dall'articolo 34[3] della LOPDGDD.

Nota 3 — Articolo 34 della LOPDGDD, «Designazione di un responsabile della protezione dei dati» (traduzione del testo di legge riportato nel documento). 1. I titolari e i responsabili del trattamento devono designare un responsabile della protezione dei dati nei casi previsti dall'articolo 37, paragrafo 1, del regolamento (UE) 2016/679 e, in ogni caso, quando si tratti dei seguenti soggetti:

a) Gli ordini professionali e i loro consigli generali.

b) Gli istituti di istruzione che erogano insegnamenti in uno qualsiasi dei livelli previsti dalla legislazione sul diritto all'istruzione, nonché le università pubbliche e private.

c) Le entità che gestiscono reti e prestano servizi di comunicazione elettronica secondo la rispettiva legislazione, quando trattino abitualmente e sistematicamente dati personali su larga scala.

d) I prestatori di servizi della società dell'informazione quando effettuino la profilazione su larga scala degli utenti del servizio.

e) I soggetti compresi nell'articolo 1 della legge 10/2014, del 26 giugno, sull'ordinamento, la vigilanza e la solvibilità degli enti creditizi.

f) Gli istituti finanziari di credito.

g) Le imprese di assicurazione e di riassicurazione.

h) Le imprese di servizi d'investimento disciplinate dalla legislazione sul mercato dei valori mobiliari.

i) I distributori e i venditori di energia elettrica nonché i distributori e i venditori di gas naturale.

j) I soggetti responsabili di archivi condivisi per la valutazione della solvibilità patrimoniale e creditizia o di archivi condivisi per la gestione e la prevenzione delle frodi, compresi i responsabili degli archivi disciplinati dalla normativa in materia di prevenzione del riciclaggio e del finanziamento del terrorismo.

k) I soggetti che svolgono attività di pubblicità e promozione commerciale, comprese le ricerche commerciali e di mercato, quando effettuino trattamenti basati sulle preferenze degli interessati o svolgano attività che comportino la loro profilazione.

l) Le strutture sanitarie legalmente obbligate a conservare le cartelle cliniche dei pazienti. Sono esclusi i professionisti sanitari che, pur essendo legalmente tenuti alla conservazione delle cartelle cliniche dei pazienti, esercitano individualmente la propria attività.

m) I soggetti che abbiano fra i propri scopi la redazione di rapporti commerciali riferibili a persone fisiche.

n) Gli operatori che esercitano attività di gioco mediante canali elettronici, informatici, telematici e interattivi, in conformità alla normativa sul gioco.

ñ) Le imprese di sicurezza privata.

o) Le federazioni sportive quando trattino dati di minori.

2. I titolari o i responsabili del trattamento non rientranti nel comma precedente possono designare volontariamente un responsabile della protezione dei dati, al quale si applica la disciplina prevista dal regolamento (UE) 2016/679 e dalla presente legge organica.

3. I titolari e i responsabili del trattamento comunicano, entro dieci giorni, all'Agenzia spagnola per la protezione dei dati o, ove competente, alle autorità regionali per la protezione dei dati, le designazioni, le nomine e le cessazioni dei responsabili della protezione dei dati, sia nei casi di designazione obbligatoria sia in quelli di designazione volontaria.

4. L'Agenzia spagnola per la protezione dei dati e le autorità regionali per la protezione dei dati tengono, ciascuna nell'ambito delle rispettive competenze, un elenco aggiornato dei responsabili della protezione dei dati, accessibile per via elettronica.

5. Nell'adempimento degli obblighi di cui al presente articolo, i titolari e i responsabili del trattamento possono stabilire che il responsabile della protezione dei dati eserciti a tempo pieno o parziale, tenendo conto, fra gli altri criteri, del volume dei trattamenti, delle categorie particolari di dati trattati o dei rischi per i diritti o le libertà degli interessati.

2. Definire il profilo del RPD

L'organizzazione deve individuare quale tipologia di RPD sia necessaria, tenendo conto di:

- **Dimensioni dell'organizzazione:** in una PMI può essere sufficiente un RPD esterno a tempo parziale. In una grande impresa, data la complessità e il volume dei trattamenti, potrebbe essere necessario un team privacy interno.
- **Complessità dei trattamenti:** se l'organizzazione tratta dati particolari o dati su larga scala, il RPD deve possedere conoscenze tecniche avanzate.

- **Settore di attività:** nei settori regolamentati (per esempio sanità, banche, istruzione) è fortemente raccomandabile che il RPD possieda competenze specifiche di settore.
- **Conoscenza dell'organizzazione.**

3. Parametri per la valutazione della posizione del RPD

Una volta individuata la necessità o l'obbligo di designare un RPD, e tenuto conto del contesto, della natura e dell'ambito dell'organizzazione, possono essere valutati i seguenti parametri:

- **Conoscenze ed esperienza:** dispone di una formazione comprovata e adeguata in materia di protezione dei dati? Ha già svolto la funzione di RPD o lavorato in ambiti affini? Conosce il settore di attività dell'organizzazione?
- **Indipendenza:** può agire senza conflitti di interessi? Ha accesso diretto all'alta direzione? Nell'organizzazione esiste un gruppo di lavoro, un'unità o personale incaricato di gestire le questioni relative alla protezione dei dati che non rientrano nei compiti propri del RPD?
- **Disponibilità:** può dedicare il tempo necessario alle funzioni del RPD? Se il RPD è esterno, il contratto assicura una disponibilità sufficiente?
- **Risorse:** l'organizzazione può fornire al RPD le risorse necessarie (strumenti, gruppo di lavoro, budget)?[4]
- **Certificazioni:** possiede una certificazione per RPD riconosciuta dal mercato oppure una certificazione in materia di privacy o ingegneria della privacy?

Nota 4. Questo aspetto è particolarmente rilevante quando il servizio di RPD è affidato a un'organizzazione esterna.

4. Designazione formale del RPD

Dopo la scelta del candidato, l'organizzazione deve formalizzare la designazione, secondo i passaggi seguenti.

Decisione di designazione. La nomina del RPD deve essere approvata dall'organo di governo dell'organizzazione. Per esempio, nel settore pubblico, dal consiglio di governo, dall'organo direttivo o dall'organo equivalente; nel settore privato, dal consiglio di amministrazione, dall'amministratore delegato, dal direttore generale oppure da una persona debitamente autorizzata mediante apposita procura speciale.

Documentazione della designazione. La designazione deve essere formalizzata per iscritto e comprendere:

a) nome e recapiti del RPD (telefono, indirizzo e-mail);

b) compiti del RPD (ai sensi dell'articolo 39 del GDPR);

c) ambito di intervento e competenze (per esempio, l'intera organizzazione o una specifica divisione), nonché eventuali ulteriori funzioni assegnate;

d) durata della nomina (se a tempo determinato);

e) risorse assegnate (budget, personale, strumenti);

f) garanzie di indipendenza (per esempio accesso diretto all'alta direzione, protezione contro le ritorsioni e ulteriori garanzie necessarie a prevenire o gestire i conflitti di interessi).

Comunicazione della designazione. L'organizzazione deve comunicare la nomina del RPD:

a) **All'AEPD**, attraverso la procedura di registrazione predisposta. Nelle comunità autonome dotate di competenze in materia di protezione dei dati, gli organismi pubblici devono comunicare la designazione alle rispettive autorità.

b) **Ai dipendenti dell'organizzazione:** la figura del RPD deve essere conosciuta da tutto il personale, soprattutto da chi tratta dati personali. Si raccomanda di indicarne il nome e i recapiti nella politica aziendale di protezione dei dati, nelle informative privacy e in luoghi condivisi, come la intranet.

c) **Agli interessati** (clienti, utenti ecc.): il RPD deve essere indicato quale punto di contatto nelle informazioni sul trattamento fornite agli interessati (per esempio, sito web, contratti, clausole informative).

d) **Pubblicazione dei recapiti del RPD:** fermo quanto sopra, l'articolo 37, paragrafo 7, del GDPR stabilisce che «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». Si raccomanda che la designazione sia accompagnata da meccanismi di comunicazione interna che consentano a tutte le aree dell'organizzazione di conoscere l'esistenza del RPD, i suoi compiti e i canali disponibili per interagire con lui. A questo scopo possono essere utilizzati il sito web, l'inventario dei trattamenti, le politiche privacy e le relative procedure o, preferibilmente, una sezione dedicata alla protezione dei dati; i registri interni, come il registro delle attività di trattamento (RAT); la documentazione legale, i contratti, le clausole informative e gli avvisi legali.

e) **Disponibilità del RPD:** la designazione formale costituisce una garanzia essenziale di trasparenza e certezza del diritto. Si raccomanda che la politica di protezione dei dati o lo stesso atto di designazione disciplini espressamente gli aspetti relativi alla continuità della funzione, in particolare in caso di assenza temporanea, sostituzione o cessazione improvvisa dall'incarico.

5. Compiti del RPD dopo la designazione

Nella pratica può accadere che alcune organizzazioni interpretino la designazione formale del RPD come il trasferimento a tale figura di tutte le responsabilità in materia di privacy e protezione dei dati. Tale interpretazione è contraria al modello di responsabilizzazione previsto dal GDPR e può determinare l'attribuzione al RPD di funzioni operative, esecutive o decisionali incompatibili con il suo ruolo consultivo e di vigilanza. In nessun caso la designazione formale del RPD può essere intesa come trasferimento delle responsabilità di conformità normativa che il GDPR e la LOPDGDD attribuiscono al titolare o al responsabile del trattamento.

Una volta designato, il RPD deve esercitare i compiti previsti dall'articolo 39 del GDPR:

- informare e fornire consulenza al titolare o al responsabile del trattamento in ordine agli obblighi applicabili;
- sorvegliare l'osservanza del GDPR, della LOPDGDD e delle altre normative settoriali applicabili;
- fornire consulenza in merito alla valutazione d'impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;
- cooperare con l'AEPD e fungere da punto di contatto con l'autorità di controllo;
- fungere da punto di contatto per gli interessati in relazione al trattamento dei loro dati.

6. Cessazione dall'incarico del RPD

Le designazioni di cui all'articolo 34 della LOPDGDD[5] ricomprendono implicitamente anche i casi di cessazione del RPD e, pertanto, l'obbligo per titolari e responsabili di comunicare all'autorità di controllo sia la nomina sia la cessazione, nonché ogni circostanza che comporti una modifica o un aggiornamento della

comunicazione precedentemente effettuata. L'assenza di una procedura effettiva può causare problemi pratici, come la permanenza di informazioni inesatte o non aggiornate sul RPD oppure l'indicazione del precedente RPD come interlocutore dell'autorità di controllo, degli interessati o di terzi, nonostante la cessazione del rapporto con l'organizzazione. Per prevenire periodi di assenza del RPD, anche transitori, una soluzione pratica efficace consiste nell'adozione di un organo collegiale (per esempio un «ufficio privacy»), che assicuri la continuità del servizio anche in caso di assenze sopravvenute.

L'articolo 36, comma 2, della LOPDGDD[6] stabilisce che il RPD non può essere rimosso dall'incarico né sanzionato dal titolare o dal responsabile del trattamento per il mero esercizio delle sue funzioni, salvo che ricorrano dolo o colpa grave. Tale previsione riveste particolare rilievo poiché evidenzia la necessità di garantirne l'indipendenza funzionale.

A questo proposito, occorre considerare che, sebbene il titolare e il responsabile debbano garantire l'indipendenza del RPD nell'esercizio delle funzioni, ciò non conferisce al RPD un regime di tutela speciale analogo a quello che il legislatore riconosce ai rappresentanti dei lavoratori o al responsabile del servizio di prevenzione dei rischi sul lavoro[7]; secondo la giurisprudenza, infatti, «non è l'indipendenza nell'esercizio di una funzione, bensì la funzione in sé a far sì che la rappresentanza legale dei lavoratori goda di una maggiore protezione contro il licenziamento e che a essa siano equiparati i delegati alla prevenzione dei rischi ai sensi dell'articolo 30, paragrafo 4, della LPRL»[8].

Nota 5. Articolo 34, comma 3, LOPDGDD: i titolari e i responsabili del trattamento comunicano entro dieci giorni all'AEPD o, secondo i casi, alle autorità regionali per la protezione dei dati le designazioni, le nomine e le cessazioni dei RPD, sia nei casi in cui la designazione sia obbligatoria sia in quelli di designazione volontaria.

Nota 6. Articolo 36, comma 2, LOPDGDD: qualora si tratti di una persona fisica inserita nell'organizzazione del titolare o del responsabile del trattamento, il RPD non può essere rimosso né sanzionato dal titolare o dal responsabile per l'esercizio delle sue funzioni, salvo che abbia agito con dolo o colpa grave. Deve essere garantita l'indipendenza del RPD all'interno dell'organizzazione, evitando qualsiasi conflitto di interessi.

Nota 7. Sentenza STSJ M 7356/2026 — ECLI:ES:TSJM:2026:7356.

Nota 8. Articolo 30, comma 4, della LPRL: i lavoratori designati non possono subire alcun pregiudizio derivante dalle attività di protezione e prevenzione dei rischi professionali in azienda. Nell'esercizio di tale funzione, essi godono, in particolare, delle garanzie previste per i rappresentanti dei lavoratori dalle lettere a), b) e c) dell'articolo 68 e dal comma 4 dell'articolo 56 del testo unico della legge spagnola sullo Statuto dei lavoratori.

7. Buone prassi nella designazione del RPD

L'EDPB e l'AEPD considerano buone prassi per garantire l'effettività della designazione del RPD almeno le seguenti:

- designare il RPD a un livello amministrativo elevato (per esempio il livello 28–30 nell'Amministrazione generale dello Stato spagnolo, per assicurare l'interlocuzione con i massimi vertici);
- formalizzare, come buona prassi organizzativa, la nomina del RPD mediante una *lettera di incarico* quando sia interno, oppure mediante un'apposita disciplina contrattuale, nel settore privato o nei capitolati degli appalti pubblici, quando il servizio sia prestato da un RPD esterno;
- prevedere in tale documento, fra gli altri aspetti, i compiti attribuiti al RPD, i meccanismi di reporting diretto agli organi direttivi, le procedure di consultazione tempestiva in materia di protezione dei dati, le risorse disponibili, le garanzie di indipendenza e il piano di intervento o vigilanza previsto per l'esercizio delle funzioni;
- inserire il RPD nell'organigramma aziendale per assicurarne la visibilità;

- istituire un ufficio o un comitato per la protezione dei dati, così da garantire la continuità della funzione anche in caso di avvicendamento o assenza del personale;
- valutare i conflitti di interessi prima della designazione;
- far designare il RPD dal consiglio di amministrazione o dalla direzione generale;
- garantire che il RPD riferisca direttamente all'alta direzione;
- evitare l'attribuzione al RPD di funzioni operative che possano generare conflitti di interessi;
- fornire risorse sufficienti (budget, strumenti e personale);
- nel caso di un RPD esterno, stipulare un contratto chiaro che definisca compiti, garanzie di indipendenza, durata del servizio e risorse assegnate.

In definitiva, la designazione deve assicurare al RPD l'accesso a tutte le informazioni necessarie per esercitare le proprie funzioni con indipendenza e deve tenere conto non soltanto delle sue qualifiche professionali, ma anche delle condizioni effettive di esercizio dei compiti e delle garanzie d'indipendenza. In tal senso, la sentenza dell'Audiencia Nacional n. 139/2026, del 18 marzo 2026 (ECLI:ES:AN:2026:1355), conferma la necessità di esaminare le funzioni concretamente attribuite alla persona designata, specialmente quando questa partecipa a decisioni che determinano finalità e mezzi dei trattamenti che successivamente è chiamata a sorvegliare (articolo 38, paragrafo 6, GDPR).

III. Indipendenza quale garanzia di efficacia

L'indipendenza del RPD è una delle garanzie fondamentali previste dall'articolo 38, paragrafo 3, del GDPR e sviluppate dalle linee guida dell'EDPB e dalle raccomandazioni[9] dell'AEPD. Essa assicura che il RPD possa esercitare i propri compiti di vigilanza, consulenza e controllo senza pressioni esterne, conflitti di interessi o influenze idonee a comprometterne l'obiettività.

Di seguito vengono esaminate le implicazioni dell'indipendenza del RPD, le modalità per garantirla e i requisiti necessari alla luce del quadro normativo e delle buone prassi raccomandate dall'AEPD e dall'EDPB.

L'articolo 38, paragrafo 3, del GDPR stabilisce che «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 RPD, pertanto, non può ricevere istruzioni sulle modalità di esercizio delle sue funzioni né essere rimosso o sanzionato per avere svolto i compiti di vigilanza e consulenza.

Il paragrafo 5 dell'articolo 38 del GDPR dispone inoltre che «Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri». Ciò rafforza l'esigenza che il RPD possa agire senza interferenze che gli impediscano di accedere a tutte le informazioni necessarie.

La LOPDGDD integra il quadro del GDPR, stabilendo che il RPD debba operare con autonomia e in assenza di conflitti di interessi (articolo 36) e vietando pressioni o influenze suscettibili di comprometterne l'indipendenza.

Le linee guida dell'EDPB sottolineano che l'indipendenza del RPD è essenziale per la sua credibilità ed efficacia: è dunque necessario che possa agire senza timore di ritorsioni e con accesso diretto ai massimi vertici dell'organizzazione, come il consiglio di amministrazione o la direzione generale. Sul piano pratico, i requisiti di indipendenza possono essere sintetizzati come segue.

Nota 9. https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-impulsa-un-modelo-comun-de-cumplimiento-en-el-sector

A. Indipendenza funzionale

- **Assenza di istruzioni in relazione ai compiti:** al RPD non può essere imposto di assumere una determinata posizione in materia di protezione dei dati. Per esempio, se identifica e valuta un rischio connesso a un trattamento, non può subire pressioni affinché lo minimizzi, lo ignori, lo eluda o riveda la propria valutazione.
- **Libertà nella formulazione di relazioni e raccomandazioni:** il RPD deve poter emettere pareri, raccomandazioni e segnalazioni senza che siano modificati o censurati dall'organizzazione. Se, per esempio, redige una relazione sull'inadempimento di obblighi relativi a una DPIA, tale relazione deve essere rispettata e presa in considerazione dalla direzione.

B. Indipendenza gerarchica

- **Collocazione nell'organigramma:** il RPD deve riferire direttamente al livello gerarchico più elevato dell'organizzazione (per esempio consiglio di amministrazione, direttore generale o comitato di direzione).

- **Settore pubblico:** il RPD deve dipendere da un organo dotato di potere decisionale (per esempio un sottosegretariato o una segreteria generale).
- **Settore privato:** deve riferire direttamente alla direzione generale o al consiglio di amministrazione. Nelle organizzazioni con organi di amministrazione e organi di direzione distinti si raccomanda che il RPD riferisca a entrambi i livelli.

C. Conflitti di interessi

- Nel settembre 2025 l'Organizzazione internazionale per la normazione (ISO)[10] ha pubblicato la norma «Conflict of interest in organizations» (ISO 37009:2025). Tale norma fornisce orientamenti generali per comprendere, identificare e gestire i conflitti di interessi in qualsiasi organizzazione, siano essi potenziali, percepiti o effettivi e possano ostacolare il perseguimento degli obiettivi dell'organizzazione o le funzioni dei suoi componenti, come nel caso del RPD.
- Un'adeguata gestione dei conflitti di interessi, coerente con la ISO 37009:2025, è fondamentale per la fiducia e la reputazione dell'organizzazione. Il suo ambito è generale e non si limita alla lotta contro la corruzione: è uno strumento essenziale per garantire l'integrità e l'efficacia di ogni processo decisionale. Di conseguenza, per prevenire i conflitti di interessi, è necessario che i titolari predispongano regole interne che consentano di individuarli e gestirli adeguatamente.
- Il GDPR ammette che il RPD sia interno o esterno all'organizzazione tenuta alla designazione. In entrambi i casi, il titolare o il responsabile del trattamento deve assicurare che funzioni e compiti del RPD non siano pregiudicati da potenziali conflitti di interessi.
- Il RPD non può svolgere funzioni suscettibili di entrare in conflitto con il suo ruolo di vigilanza. Il conflitto può emergere in fase di designazione, durante lo svolgimento dei compiti, nell'esercizio di altri ruoli attribuiti dal titolare o in qualsiasi altro momento.

Sono esempi di conflitti di interessi:

- essere responsabile di un ufficio che tratta dati personali (per esempio direttore marketing, risorse umane o IT);
- svolgere funzioni che attribuiscano potere decisionale nella determinazione o approvazione delle finalità e dei mezzi dei trattamenti o delle relative operazioni (per esempio assumere la decisione definitiva sull'installazione e configurazione di un sistema di videosorveglianza).

Quale elemento fondamentale del principio di responsabilizzazione, si raccomanda che l'organizzazione disponga, prima della nomina del RPD, di regole per individuare i conflitti di interessi concretamente ipotizzabili, definire come affrontare le situazioni non previste e stabilire come gestirle.

Nota 10. ISO (International Organization for Standardization): organismo indipendente e non governativo che riunisce esperti di oltre 160 Paesi per elaborare norme internazionali finalizzate a garantire qualità, sicurezza, efficienza e compatibilità di prodotti, servizi e sistemi.

D. Indipendenza economica

L'adeguatezza delle risorse è un presupposto essenziale per il corretto svolgimento dei compiti del RPD. La valutazione di tali risorse deve tuttavia essere effettuata considerando dimensioni, complessità e caratteristiche di ciascuna organizzazione.

Anche l'autonomia finanziaria è essenziale per l'indipendenza effettiva del RPD, poiché la sua assenza può limitarne, per esempio, l'accesso a una formazione adeguata, a strumenti di supporto o all'assistenza specialistica di esperti esterni. In generale:

- il RPD deve disporre di un compenso adeguato e di stabilità nell'incarico, per prevenire pressioni economiche;
- non può essere rimosso per l'esercizio delle funzioni (articolo 38, paragrafo 3, GDPR); l'eventuale rimozione deve essere giustificata da un possibile inadempimento grave dei propri obblighi e non da un dissenso rispetto all'organizzazione. La prospettiva della rimozione può infatti configurare una pressione implicita sul piano della retribuzione e della stabilità;
- non deve avere interessi rilevanti o di controllo nei trattamenti dai quali possa ricavare vantaggi economici. Per esempio, potrebbe risultare compromessa la sua indipendenza se fosse socio di maggioranza di un'impresa che presta servizi di trattamento dei dati alla propria organizzazione. Anche bonus o compensi variabili legati ai risultati economici o agli utili societari potrebbero incidere sull'obiettività.

E. Indipendenza organizzativa

L'assetto organizzativo non può ostacolare o impedire lo svolgimento dei compiti del RPD. La sua collocazione deve garantire:

- accesso effettivo a tutti i dati, processi e sistemi necessari per l'esercizio delle funzioni, per esempio registri delle attività di trattamento (RAT), valutazioni d'impatto e contratti con i responsabili del trattamento;
- disponibilità delle risorse messe a disposizione dall'organizzazione: risorse umane (personale di supporto, ove necessario), risorse tecniche (strumenti di analisi, software gestionali ecc.) e budget per formazione e assistenza esterna, se necessaria (consulenza legale e tecnica);
- coinvolgimento e partecipazione nelle decisioni strategiche: il RPD deve essere consultato tempestivamente nei progetti che comportano trattamenti di dati personali (articolo 38, paragrafo 1, GDPR). Per esempio, deve prestare la propria consulenza nella fase di progettazione di un nuovo sistema di intelligenza artificiale che tratti dati personali.

Le raccomandazioni dell'AEPD per il settore pubblico propongono:

- l'inserimento del RPD nella struttura organizzativa a un livello amministrativo elevato (per esempio livelli 28–30);
- la pubblicità e la documentazione trasparente della designazione formale, con una descrizione chiara di funzioni e limiti;
- l'istituzione di strutture stabili, quali uffici o comitati privacy, per assicurare la continuità della funzione anche in caso di cambiamenti del personale;
- la valutazione dei conflitti di interessi prima della designazione.

Nel settore privato il RPD può essere nominato dal consiglio di amministrazione o dal direttore generale. Se esterno, può essere designato mediante un contratto specifico che ne garantisca l'indipendenza e l'assenza di istruzioni nell'esercizio delle funzioni, attraverso apposite clausole.

Una buona prassi, tanto nel settore pubblico quanto in quello privato, consiste nell'elaborazione da parte del RPD di una relazione annuale destinata all'alta direzione sul livello di conformità in materia di protezione dei dati, che non possa essere modificata o censurata.

Un'altra buona prassi consiste nell'includere, nell'ambito degli audit privacy, la verifica dell'indipendenza del RPD.

Il RPD deve poter accedere al canale interno di segnalazione degli illeciti, attraverso il quale comunicare eventuali pressioni o possibili conflitti di interessi che incidano o possano incidere sulla sua indipendenza nell'esercizio delle funzioni.

IV. Reporting e rendicontazione del RPD

L'AEPD ritiene una buona prassi promuovere meccanismi di reporting del RPD adeguati alle caratteristiche di ciascuna organizzazione, tali da assicurare una comunicazione efficace con i massimi vertici, senza tuttavia prescrivere un modello specifico o generalizzato. Qualunque modello prescelto deve garantire la separazione fra le funzioni consultive e di vigilanza del RPD e la sua indipendenza rispetto a ogni funzione che comporti poteri decisionali sui trattamenti di dati personali.

Tale orientamento trova un sostegno particolarmente diretto nella relazione dell'EDPB del gennaio 2024 sull'azione coordinata relativa alla designazione e alla posizione dei RPD. Il paragrafo 4.6 individua difficoltà di accesso all'alta direzione e contempla espressamente l'elaborazione di raccomandazioni o modelli adattabili di reporting, anche annuale, quali possibili buone prassi istituzionali.

Nella stessa direzione, la CNIL francese, mediante la guida e il modello di relazione di attività pubblicati il 27 aprile 2026, ha predisposto uno strumento per il monitoraggio dell'attività e la comunicazione con la direzione, raccomandandone l'uso senza qualificarlo come giuridicamente obbligatorio. Entrambi i documenti sostengono l'opportunità di promuovere sistemi di reporting proporzionati e utili, preservando la flessibilità organizzativa ed evitando che la documentazione diventi un fine a sé stante.

Il reporting del RPD quale strumento di governance e responsabilizzazione

Il reporting o la rendicontazione del RPD deve essere strutturato in funzione dell'assetto, delle dimensioni e della complessità dell'organizzazione, del suo settore di attività e della disciplina applicabile. Costituisce una diretta espressione del principio di responsabilizzazione e una condizione necessaria per l'effettività dei compiti minimi attribuiti al RPD dal GDPR. Benché il GDPR non prescriva una relazione annuale né stabilisca un modello formale di rendicontazione periodica, esso richiede che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati, abbia accesso alle informazioni necessarie per esercitare le funzioni e riferisca direttamente al vertice gerarchico dell'organizzazione[11].

Tali prescrizioni devono tradursi in meccanismi effettivi di interlocuzione fra il RPD e gli organi direttivi, che consentano di comunicare rischi, raccomandazioni, esigenze di conformità e questioni rilevanti per la protezione dei dati[12]. La finalità non è aumentare gli oneri documentali dell'organizzazione o del RPD, bensì assicurare alla direzione le informazioni necessarie per assumere decisioni consapevoli e poter dimostrare l'effettiva partecipazione del RPD alla governance dei dati personali.

A. Meccanismi di reporting proporzionati alle dimensioni e alla complessità dell'organizzazione

Non esiste un unico modello valido di reporting del RPD, conclusione coerente tanto con l'assenza di disposizioni specifiche del GDPR sui formati, quanto con la varietà delle soluzioni presenti negli orientamenti della CNIL, dell'autorità finlandese, dell'autorità irlandese e del Garante europeo della protezione dei dati (EDPS).

I meccanismi di comunicazione e rendicontazione devono adattarsi alla natura, alle dimensioni, alla complessità e al livello di rischio dei trattamenti effettuati da ogni organizzazione, in attuazione del principio generale di responsabilizzazione e, in particolare, dell'approccio basato sul rischio proprio del GDPR.

Nelle organizzazioni di grandi dimensioni, con strutture complesse, trattamenti intensivi di dati personali o attività che comportano rischi significativi per i diritti e le libertà delle persone, può essere opportuno

predisporre meccanismi periodici e formalizzati di reporting, anche attraverso relazioni strutturate destinate all'alta direzione[13]. Nelle organizzazioni più piccole, o con trattamenti meno complessi, la tracciabilità dell'attività del RPD può essere assicurata attraverso strumenti più semplici, quali verbali di riunione, comunicazioni documentate, registri delle raccomandazioni o relazioni specifiche su questioni rilevanti[14].

Il criterio decisivo non dovrebbe essere la presenza di un determinato documento, bensì la capacità di dimostrare che il RPD ha potuto esercitare le proprie funzioni, formulare raccomandazioni e comunicare ai vertici i rischi e gli incidenti rilevanti individuati.

Nota 11. Articoli 38 e 39 del GDPR; linee guida WP243/EDPB; guida dell'EDPS sul ruolo del DPO nelle istituzioni e negli organismi dell'Unione europea.

Nota 12. Linee guida WP243/EDPB; azione coordinata di enforcement dell'EDPB sulla designazione e sulla posizione del DPO; guida EDPS 2025.

Nota 13. Per esempio il modello CNIL: https://www.cnil.fr/fr/rapport-activite-dpo

Nota 14. Orientamenti delle autorità finlandese e irlandese e modelli professionali del BvD.

B. Comunicazione diretta con l'alta direzione

L'obbligo di riferire direttamente al vertice gerarchico più elevato, previsto dall'articolo 38, paragrafo 3, del GDPR, deve essere interpretato quale garanzia sostanziale di indipendenza e non come mera previsione formale dell'organigramma. Le organizzazioni devono predisporre canali stabili affinché il RPD possa comunicare direttamente ai vertici le questioni rilevanti in materia di conformità, senza filtri indebiti, ostacoli o intermediari[15].

È particolarmente raccomandabile definire internamente le procedure di escalation dei rischi, le modalità di comunicazione degli incidenti significativi e i meccanismi di monitoraggio delle raccomandazioni del RPD. In generale, l'effettività della funzione dipende in larga misura da un'interlocuzione reale con gli organi direttivi e dalla capacità di formulare segnalazioni o raccomandazioni prima della concretizzazione dei rischi.

Si raccomanda inoltre di integrare il quadro di esercizio delle funzioni del RPD nel procedimento di designazione e di definirlo nella politica di protezione dei dati del titolare, individuando compiti, ambito d'intervento, risorse, garanzie di indipendenza e canali di reporting. Restano ferme le eventuali relazioni periodiche, le comunicazioni straordinarie necessarie in presenza di violazioni rilevanti dei dati o di rischi elevati e le attività presso l'autorità di controllo.

C. Documentazione della consulenza e tracciabilità delle decisioni

Una delle garanzie più efficaci per rafforzare l'indipendenza e l'utilità del RPD è l'adeguata documentazione delle attività di consulenza e vigilanza. Non si tratta di generare oneri documentali superflui, bensì di assicurare una ragionevole tracciabilità delle questioni rilevanti, in modo da comprovare l'intervento del RPD e il rispetto degli obblighi di responsabilizzazione. Si raccomanda perciò di conservare evidenze sufficienti relative a:

- richieste di consulenza rilevanti rivolte al RPD;
- pareri e consulenze resi;
- raccomandazioni formulate;
- decisioni adottate dall'organizzazione su questioni rilevanti per la protezione dei dati;
- attività di vigilanza svolte.

Nota 15. Linee guida WP243/EDPB; guida EDPS 2025; azione coordinata di enforcement dell'EDPB.

L'esperienza comparata europea evidenzia inoltre una crescente tendenza a documentare i casi in cui l'organizzazione decide di discostarsi dal parere del RPD. Si tratta di una prassi particolarmente utile per rafforzare la tracciabilità del processo decisionale e agevolare la rendicontazione, senza modificare il carattere non vincolante delle raccomandazioni del RPD.

D. Comunicazione di rischi, incidenti e violazioni rilevanti

Il reporting del RPD non deve limitarsi alle comunicazioni periodiche, poiché talune circostanze richiedono una comunicazione immediata agli organi di amministrazione e direzione. A tale proposito, l'articolo 36, comma 4, della LOPDGDD prevede espressamente l'obbligo di documentare e comunicare le violazioni rilevanti in materia di protezione dei dati. Tale previsione rispecchia un principio più ampio: la direzione deve essere tempestivamente informata delle situazioni suscettibili di compromettere in modo significativo la conformità normativa, la tutela dei diritti degli interessati o la stessa posizione dell'organizzazione[16].

Si raccomanda pertanto che i meccanismi interni consentano al RPD di portare immediatamente all'attenzione dei vertici rischi significativi, inadempimenti rilevanti, carenze strutturali o esigenze organizzative che richiedano l'intervento della direzione.

E. Relazioni periodiche sull'attività quale buona prassi avanzata

La redazione di relazioni periodiche sull'attività costituisce una buona prassi di governance particolarmente utile nelle organizzazioni complesse, ma non un obbligo giuridico generale derivante dal GDPR.

L'iniziativa[17] della CNIL francese, che ha pubblicato una guida specifica e un modello di relazione sull'attività del DPO, costituisce un riferimento di particolare valore per le organizzazioni che intendano rafforzare i propri meccanismi di governance e rendicontazione.

Tali relazioni possono offrire una visione strutturata dello stato di conformità dell'organizzazione, agevolare la pianificazione delle attività future e assicurare la continuità della funzione del RPD.

Si raccomanda che gli eventuali modelli di relazione siano concepiti per facilitare il processo decisionale della direzione e non per produrre documentazione meramente formale. Il contenuto dovrebbe essere proporzionato alle caratteristiche dell'organizzazione e concentrarsi sui principali rischi, sulle attività svolte, sulle raccomandazioni formulate e sulle esigenze individuate.

Nota 16. Tale previsione dell'articolo 36, comma 4, LOPDGDD trova ulteriore sostegno nelle linee guida WP243/EDPB, nella guida EDPS 2025 e nei documenti CNIL.

Nota 17. Articoli 38 e 39 del GDPR; modello CNIL sul *rapport d'activité du DPO*.

Risorse organizzative necessarie per un reporting efficace

La rendicontazione del RPD può essere efficace soltanto se l'organizzazione garantisce le condizioni necessarie per esercitare le funzioni. I meccanismi di reporting, così come le risorse e i mezzi messi a disposizione, devono essere valutati alla luce delle specificità di ogni organizzazione, comprese dimensioni, natura, struttura, volume dei trattamenti e complessità.

Tali garanzie non mirano ad aumentare gli obblighi documentali, bensì ad assicurare che il RPD possa svolgere un'effettiva attività di vigilanza e sottoporre tempestivamente alla direzione, nelle forme opportune, le questioni che ne richiedono l'attenzione.

L'obiettivo del sistema europeo non consiste nell'imporre modelli uniformi di reporting o relazioni periodiche obbligatorie, ma nel garantire una comunicazione effettiva, documentata e proporzionata fra

RPD e alta direzione. Le concrete modalità possono variare in funzione delle caratteristiche dell'organizzazione. Ciò che conta è la possibilità di dimostrare l'effettiva partecipazione del RPD, l'adeguata considerazione delle sue raccomandazioni e l'integrazione della protezione dei dati nei processi decisionali e di governance dell'ente.

V. Garanzie organizzative relative alla nomina, alla permanenza nell'incarico e alla cessazione

A. Designazione formale del RPD quale garanzia di indipendenza istituzionale

La designazione del RPD non è un mero adempimento organizzativo, ma una garanzia istituzionale essenziale per l'effettività del sistema di protezione dei dati. L'obbligo di designazione nei casi di cui all'articolo 37 del GDPR deve essere interpretato congiuntamente agli articoli 38 e 39. La finalità non è semplicemente individuare una persona incaricata di determinate funzioni, bensì garantire che l'organizzazione disponga di un interlocutore specializzato, indipendente e adeguatamente integrato nei processi di governance.

La nomina del RPD dovrebbe pertanto essere sempre formalizzata con un atto espresso, scritto e sufficientemente documentato, indipendentemente dall'esistenza di procedure interne specifiche.

Si raccomanda in particolare che l'atto identifichi:

- la persona fisica o l'entità designata;
- la data di decorrenza della nomina;
- la collocazione organizzativa del RPD;
- i canali di reporting;
- i mezzi e le risorse inizialmente assegnati;
- le modalità di accesso all'alta direzione.

Tale orientamento è coerente con gli articoli 34–37 della LOPDGDD, con i requisiti organizzativi degli articoli 38 e 39 del GDPR, con le linee guida WP243 sui RPD recepite dall'EDPB, con l'azione coordinata dell'EDPB sulla designazione e sulla posizione del DPO e con la guida dell'EDPS sul ruolo dei responsabili della protezione dei dati.

L'esperienza europea comparata evidenzia inoltre la tendenza a integrare l'atto formale di nomina con documenti che definiscano espressamente funzioni, responsabilità, collocazione organizzativa e meccanismi di reporting, come risulta dal documento di indirizzo del Garante italiano del 2021 e dai criteri dell'autorità olandese sulla posizione istituzionale del *functionaris gegevensbescherming* (FG). Sebbene tale prassi non costituisca attualmente un obbligo giuridico generale, l'AEPD ritiene che rappresenti una garanzia particolarmente adeguata per prevenire successive controversie sull'estensione dei compiti del RPD e sulla sua posizione nell'organizzazione.

B. Partecipazione del RPD alle decisioni che incidono sulla sua posizione istituzionale

L'adeguato e tempestivo coinvolgimento del RPD, attraverso consulenza e vigilanza, in tutte le questioni relative alla protezione dei dati è espressamente richiesto dall'articolo 38, paragrafo 1, del GDPR. Tale garanzia deve estendersi anche alle decisioni organizzative che incidono direttamente sulla posizione, sui compiti, sulla struttura di supporto o sulla capacità d'intervento dello stesso RPD.

Particolarmente rilevante è, al riguardo, il criterio espresso dall'AEPD nel parere giuridico n. 0038/2023, secondo il quale, quando una riorganizzazione interna incide sulle funzioni o sulla posizione istituzionale del RPD, è opportuno acquisirne preventivamente il parere. Pur non essendo vincolante, l'organizzazione deve comunque continuare a garantire l'effettiva osservanza dei requisiti del GDPR relativi alla posizione e alle funzioni del RPD.

È altresì raccomandabile documentare sia l'analisi svolta sia le ragioni della decisione definitiva, qualora questa si discosti dal parere del RPD. Tale raccomandazione trova sostegno nel citato parere AEPD n. 0038/2023, negli orientamenti dell'autorità irlandese sulla governance e sulla tracciabilità della consulenza del DPO, nelle raccomandazioni dell'autorità finlandese e nei recenti sviluppi della CNIL sul reporting e sulla rendicontazione del DPO.

Questa prassi non rende vincolanti le raccomandazioni del RPD e non trasferisce su di lui le responsabilità del titolare o del responsabile del trattamento; promuove invece la trasparenza del processo decisionale e la dimostrazione della conformità.

La raccomandazione trova specifico sostegno nelle linee guida sul RPD del Gruppo di lavoro Articolo 29 (WP243 rev.01), recepite dall'EDPB, e nel parere giuridico AEPD n. 0038/2023, che esamina sia la necessità di documentare le ragioni del mancato recepimento del consiglio del RPD sia il suo coinvolgimento nelle riorganizzazioni che ne incidono su posizione e funzioni (pp. 26 e 29). La Data Protection Commission irlandese, nella decisione del 10 maggio 2021 relativa al Department of Employment Affairs and Social Protection (IN-18-12-01, paragrafi da 6.8 a 6.13, in particolare 6.10), ritiene che un adeguato coinvolgimento del RPD richieda un'effettiva considerazione della sua consulenza e richiama la raccomandazione di documentare le ragioni per cui non viene seguita. Il modello di relazione di attività pubblicato dalla CNIL nel 2026 costituisce, infine, uno strumento complementare per sistematizzare il monitoraggio delle raccomandazioni e delle decisioni.

C. Indipendenza del RPD quale principio informatore del suo statuto giuridico

Il nucleo dello statuto giuridico del RPD non risiede nell'attribuzione di un'assoluta inamovibilità, ma nella tutela effettiva della sua indipendenza funzionale. Gli articoli 38, paragrafi 1, 2 e 3, del GDPR, letti congiuntamente al considerando 97, devono essere intesi come un insieme di garanzie volte ad assicurare che il RPD possa svolgere i compiti di vigilanza, consulenza e controllo senza ricevere istruzioni sul contenuto della propria attività e senza subire conseguenze sfavorevoli per l'esercizio delle funzioni.

Tale lettura è coerente con le linee guida WP243 rev.01, successivamente recepite dall'EDPB, con la guida EDPS sul ruolo del DPO nelle istituzioni europee e con le prassi convergenti di numerose autorità europee, fra cui la CNIL francese, l'autorità belga per la protezione dei dati, l'autorità danese e quella svedese, che attribuiscono particolare importanza all'indipendenza funzionale quale presupposto per il corretto esercizio dell'incarico. Ogni interpretazione dello statuto giuridico del RPD deve pertanto fondarsi su tale principio generale.

D. Tutela contro la rimozione dall'incarico e le misure sanzionatorie

L'articolo 38, paragrafo 3, del GDPR stabilisce che il RPD non può essere rimosso o sanzionato per l'adempimento dei propri compiti. Tale garanzia è stata interpretata dalla Corte di giustizia dell'Unione europea nelle sentenze *Leistritz*, del 22 giugno 2022 (C-534/20, ECLI:EU:C:2022:495), *X-FAB Dresden*, del 9 febbraio 2023 (C-453/21, ECLI:EU:C:2023:79) e *KISA*, del 9 febbraio 2023 (C-560/21, ECLI:EU:C:2023:81).

Nella sentenza *Leistritz*, la Corte ha precisato che il divieto previsto dall'articolo 38, paragrafo 3, del GDPR tutela il RPD contro le decisioni che pongano fine alle sue funzioni, gli siano sfavorevoli o costituiscano una sanzione, purché collegate all'esercizio dei compiti affidatigli. Tale protezione non comporta un'inamovibilità assoluta e non impedisce l'adozione di decisioni legittime fondate su ragioni estranee all'esercizio delle funzioni.

Le sentenze *Leistritz*, *X-FAB Dresden* e *KISA* confermano inoltre che il diritto nazionale può prevedere garanzie rafforzate contro la rimozione del RPD, compresa la necessità di una causa grave, purché esse non

pregiudichino gli obiettivi del GDPR. Tale giurisprudenza sostiene un'interpretazione effettiva dell'indipendenza funzionale del RPD e l'opportunità che ogni decisione di cessazione sia giustificabile mediante circostanze oggettive, distinte dall'esercizio indipendente delle funzioni.

Alla luce di tale giurisprudenza, qualsiasi misura che incida negativamente sulla posizione professionale del RPD deve poter essere giustificata da ragioni oggettive estranee all'esercizio dei compiti di vigilanza, consulenza o controllo. La tutela di cui all'articolo 38, paragrafo 3, del GDPR deve essere interpretata in termini funzionali e non meramente formali.

E. Garanzie rafforzate di permanenza nell'incarico

L'articolo 36, comma 2, della LOPDGDD rappresenta una delle espressioni più rilevanti della protezione rafforzata del RPD nel contesto europeo: quando il RPD è una persona fisica inserita nell'organizzazione, la rimozione o la sanzione può essere giustificata soltanto in presenza di dolo o colpa grave nell'esercizio delle funzioni. Tale previsione deve essere interpretata quale garanzia istituzionale diretta a tutelare l'indipendenza del RPD contro pressioni organizzative derivanti dal contenuto delle sue attività o raccomandazioni.

Le sentenze *Leistritz* (C-534/20) e *X-FAB Dresden* (C-453/21) hanno espressamente confermato che gli Stati membri possono stabilire livelli di tutela superiori a quelli previsti dal GDPR, purché non ne compromettano gli obiettivi. La possibilità di una protezione rafforzata costituisce quindi un elemento legittimo e compatibile con il modello europeo di governance della protezione dei dati.

L'esperienza comparata dimostra che alcuni ordinamenti hanno sviluppato meccanismi ancora più intensi di stabilità funzionale. Spicca il modello tedesco, nel quale la BDSG subordina la revoca del RPD all'esistenza di una causa grave e rinvia, per analogia, all'articolo 626 del codice civile tedesco (BGB), relativo alla risoluzione straordinaria di rapporti giuridici fondati su un particolare vincolo fiduciario. Si aggiunge una tutela ulteriore contro determinate decisioni successive che incidano sulla continuità del rapporto di lavoro. Sebbene tali soluzioni discendano da specifiche scelte normative nazionali, dimostrano che il rafforzamento delle garanzie di permanenza nell'incarico costituisce una via legittima per consolidare l'indipendenza effettiva del RPD. Le garanzie non implicano tuttavia un'inamovibilità assoluta né limitano la capacità organizzativa dell'ente quando sussistano cause legittime estranee all'esercizio delle funzioni.

F. Motivazione delle decisioni che incidono sul RPD

Ogni decisione che incida in modo significativo sulla posizione istituzionale del RPD dovrebbe essere adeguatamente motivata e documentata. Il GDPR non contiene un obbligo espresso di motivazione di tali decisioni. L'AEPD ritiene tuttavia che tale esigenza rappresenti un ragionevole criterio interpretativo desumibile dalla garanzia d'indipendenza prevista dall'articolo 38 del GDPR, dall'interpretazione ampia fornita dalla Corte di giustizia nella sentenza *Leistritz* sulle misure sfavorevoli, dalla tutela rafforzata di cui all'articolo 36, comma 2, della LOPDGDD e dagli obblighi generali di responsabilizzazione e rendicontazione che ispirano il sistema europeo di protezione dei dati.

Questo criterio trova inoltre sostegno nel parere giuridico AEPD n. 0038/2023 e negli orientamenti delle autorità irlandese e finlandese, che insistono sulla necessità di documentare le ragioni per le quali l'organizzazione decide di discostarsi dal parere espresso dal RPD.

Quando l'organizzazione adotta decisioni relative a nomina, permanenza, funzioni, risorse o posizione istituzionale del RPD, è pertanto raccomandabile che dia espressamente conto delle ragioni che le giustificano. Tale prassi favorisce la trasparenza, agevola il successivo controllo di legittimità e rafforza la fiducia nell'indipendenza della funzione.

G. Tutela contro le misure organizzative che incidono sostanzialmente sull'indipendenza del RPD

La tutela dell'indipendenza del RPD riconosciuta dall'articolo 38, paragrafo 3, del GDPR non deve essere valutata esclusivamente con riguardo alla cessazione formale dall'incarico. L'interpretazione ampia della Corte di giustizia nella sentenza *Leistritz*, il criterio espresso dall'AEPD nel parere n. 0038/2023, i risultati dell'azione coordinata dell'EDPB sulla designazione e la posizione del DPO e gli orientamenti olandesi sulla posizione istituzionale del FG consentono di sostenere che talune misure organizzative possono pregiudicare l'indipendenza del RPD anche senza determinarne formalmente la rimozione.

Non esiste attualmente una categoria giuridica consolidata di «rimozione occulta» o «destituzione sostanziale». Può tuttavia affermarsi che determinate decisioni organizzative debbano essere valutate con particolare attenzione alla luce delle garanzie di indipendenza previste dall'articolo 38, paragrafi 1, 2 e 3, del GDPR. Vi rientrano, fra le altre:

- la sottrazione sostanziale di compiti propri del RPD;
- la perdita dell'accesso diretto all'alta direzione;
- la riduzione significativa delle risorse indispensabili all'esercizio delle funzioni;
- la soppressione di strutture di supporto necessarie per l'effettivo svolgimento della funzione;
- la riassegnazione di competenze essenziali ad altri organi;
- ogni altra misura che svuoti sostanzialmente di contenuto i compiti attribuiti al RPD.

In tali ipotesi le organizzazioni dovrebbero valutare espressamente l'impatto della misura sull'indipendenza e sulla capacità d'intervento del RPD e documentare le ragioni dell'adozione.

H. Tutela contro le ritorsioni e garanzie organizzative minime

L'indipendenza del RPD richiede una protezione effettiva non soltanto contro la rimozione o la sanzione per l'adempimento dei compiti attribuiti dal GDPR, ma anche contro altre decisioni sfavorevoli adottate quale reazione al legittimo esercizio delle funzioni. Tale interpretazione trova sostegno nell'articolo 38, paragrafo 3, del GDPR, nella sentenza *Leistritz* (C-534/20) e nelle linee guida WP243 rev.01 del Gruppo di lavoro Articolo 29, recepite dall'EDPB.

L'autorità belga per la protezione dei dati precisa particolarmente tale garanzia negli orientamenti sull'indipendenza del RPD aggiornati il 24 gennaio 2024. Essa spiega che la protezione comprende misure pregiudizievoli per la carriera professionale, come ritardi nelle promozioni, diniego di benefici o minacce di decisioni sfavorevoli connesse all'esercizio delle funzioni. Si tratta di una tutela contro le ritorsioni, non di un divieto generale di adottare decisioni lavoristiche legittime per cause estranee all'attività di RPD.

La relazione dell'EDPB sull'azione coordinata relativa alla designazione e alla posizione dei RPD, adottata nel gennaio 2024, individua inoltre, al paragrafo 4.5.2, le ingerenze derivanti da istruzioni, rapporti contrattuali o dipendenza dal budget. Fra le raccomandazioni figurano la formalizzazione delle condizioni di esercizio della funzione e la possibilità di conservare evidenze delle interferenze subite.

Tali orientamenti, unitamente alle garanzie in tema di risorse, autonomia e reporting diretto di cui all'articolo 38 del GDPR, giustificano la raccomandazione che le organizzazioni adottino misure per prevenire le ritorsioni e consentire al RPD di svolgere i compiti in modo effettivo e indipendente. Gli orientamenti della CNIL e delle autorità danese e svedese sull'indipendenza del RPD costituiscono un ulteriore sostegno istituzionale.

Per rendere effettiva tale tutela, le organizzazioni dovrebbero assicurare stabilmente almeno:

- accesso diretto ai massimi vertici;
- risorse umane e materiali sufficienti;
- accesso alle informazioni necessarie all'esercizio dei compiti;
- supporto organizzativo adeguato;
- formazione continua;
- reale possibilità di sottoporre rischi, osservazioni e opinioni divergenti agli organi competenti.

Queste garanzie organizzative non sono elementi accessori, ma condizioni indispensabili per salvaguardare l'indipendenza effettiva del RPD e assicurare il corretto funzionamento del sistema di conformità in materia di protezione dei dati.

VI. Il RPD e la vigilanza sul principio di responsabilizzazione

Alcuni degli obblighi che il GDPR attribuisce implicitamente al titolare, con il coinvolgimento tempestivo e adeguato del RPD, non danno luogo a conflitto di interessi nella misura in cui il RPD non disponga di potere decisionale sulle decisioni definitive del titolare relative alle finalità e ai mezzi del trattamento.

Sussiste invece un conflitto di interessi manifesto quando il RPD ricopre posizioni che gli consentano di determinare, o influenzare in modo determinante, le finalità e i mezzi del trattamento dei dati personali.

Poiché la definizione di finalità e mezzi spetta esclusivamente al titolare del trattamento, il RPD non può ricoprire incarichi operativi o decisionali che debba poi essere chiamato a vigilare egli stesso.

A. Politiche di protezione dei dati

Può accadere che il titolare o il responsabile del trattamento elabori politiche di protezione dei dati per adempiere all'articolo 24 del GDPR senza richiedere la consulenza del RPD e senza considerare possibili conflitti di interessi. Considerata la conoscenza che il RPD ha dell'organizzazione, dei suoi processi e delle operazioni di trattamento, è essenziale il suo apporto consultivo affinché il titolare possa decidere l'elaborazione delle politiche previste dall'articolo 24 del GDPR, sulle quali il RPD eserciterà successivamente la funzione di vigilanza. In tale ambito, il RPD costituisce una garanzia per il funzionamento istituzionale o societario, contribuendo a politiche che migliorino l'efficienza complessiva e la fiducia dei terzi nell'organizzazione.

Come già indicato, il RPD può fornire consulenza al titolare o al responsabile nella valutazione della necessità di elaborare politiche di protezione dei dati e nel processo di predisposizione delle stesse; sarà poi incaricato di sorvegliarne l'applicazione, individuarne le carenze e suggerire eventuali miglioramenti.

Per dimostrare che il RPD è stato coinvolto adeguatamente e tempestivamente, il titolare o il responsabile devono disporre di strumenti che consentano di documentare la richiesta della sua consulenza. Tali strumenti devono anche indicare gli aspetti per i quali il titolare o il responsabile non hanno recepito le raccomandazioni del RPD, esponendone chiaramente le ragioni. Un modo per comprovare l'attività del RPD consiste nelle relazioni da questi redatte, secondo quanto indicato nel WP243, che riportino un riepilogo delle attività di consulenza e vigilanza svolte, con il dettaglio delle comunicazioni trasmesse al titolare.

Oltre alla funzione consultiva, l'articolo 39 del GDPR impone al RPD di vigilare su tali politiche[18], compresa l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale impegnato nei trattamenti, nonché gli audit pertinenti.

Un titolare che impartisca istruzioni al RPD affinché elabori, approvi o aggiorni una politica di protezione dei dati sulla quale il medesimo RPD deve vigilare violerebbe il principio di indipendenza e genererebbe un conflitto di interessi. La politica privacy deve contemplare meccanismi concreti ed efficaci che dimostrino il coinvolgimento del RPD e la fruizione della sua consulenza. Tuttavia, spetta al titolare stabilire tali meccanismi[19] e le modalità di attuazione all'interno dell'organizzazione. Il RPD ne verificherà il funzionamento nell'ambito degli audit privacy o quando necessario.

Nota 18. L'articolo 39, paragrafo 1, lettera b), del GDPR include fra i compiti minimi del RPD la sorveglianza dell'osservanza del regolamento, delle altre disposizioni dell'Unione o degli Stati membri in materia di protezione dei dati e delle politiche del titolare o del responsabile del trattamento, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti, e i relativi audit.

Nota 19. Guida «Gestione del rischio e valutazione d'impatto nei trattamenti di dati personali»: il governo o la governance dei dati è il processo mediante il quale vengono attuate politiche e procedure per garantire una gestione

efficace ed efficiente delle informazioni all'interno dell'ente. Tali politiche si applicano alla gestione di ciascun trattamento specifico.

B. Predisposizione e aggiornamento del registro delle attività di trattamento (RAT) e dell'inventario delle attività di trattamento

L'articolo 30 del GDPR impone al titolare e al responsabile di tenere aggiornato il registro delle proprie attività di trattamento. Il registro non è un mero adempimento formale, ma uno strumento dinamico ed essenziale per attuare il principio di responsabilizzazione.

Una gestione carente del RAT comporta la perdita del controllo operativo e determina rischi critici di conformità: carenza di trasparenza, valutazioni d'impatto e analisi del rischio inesistenti o inadeguate, lacune nella protezione dei dati fin dalla progettazione e per impostazione predefinita ecc. Oltre al contenuto minimo previsto dalla legge, il RPD può includere informazioni essenziali per un'adeguata gestione tecnico-organizzativa e per il miglioramento operativo dei trattamenti, quali:

- unità organizzativa responsabile delle informazioni e relativi referenti;
- informazioni sui sistemi informativi necessari alle operazioni di trattamento e relativi referenti;
- identità dei responsabili dei sistemi informativi;
- recapiti dei responsabili dei sistemi informativi;
- informazioni operative da utilizzare in caso di violazione dei dati personali;
- recapiti dell'unità di sicurezza dei sistemi informativi o del responsabile della sicurezza delle informazioni;
- procedura generale di intervento in caso di violazioni della sicurezza;
- informazioni sui responsabili del trattamento;
- procedura per la modifica delle operazioni di trattamento e la loro registrazione nel RAT;
- altri elementi pertinenti.

In definitiva, il RAT è uno strumento di lavoro che costituisce il punto di partenza essenziale per la descrizione documentata delle attività e delle operazioni di trattamento.

Questo consente di intraprendere le ulteriori azioni di conformità eventualmente necessarie in funzione delle singole fattispecie.

Inoltre, alla luce di quanto detto e della conoscenza che il RPD possiede dell'organizzazione, il suo coinvolgimento concreto nella gestione del RAT gli consente di identificare dettagli delle operazioni di trattamento che vanno oltre la mera osservanza formale dell'articolo 30 del GDPR e dell'articolo 31 della LOPDGDD. Per esempio, può mettere in relazione le operazioni di trattamento con l'utilizzo di agenti e assistenti di intelligenza artificiale nei processi dell'organizzazione, aspetto necessario per determinare il rischio intrinseco delle operazioni e i conseguenti obblighi di conformità del titolare, sui quali il RPD eserciterà i propri compiti di vigilanza, anche mediante la DPIA.

Considerato che il RAT deve essere messo a disposizione dell'autorità di controllo (articolo 30, paragrafo 4, GDPR) e che il RPD funge da punto di contatto fra titolare e autorità, il titolare o il responsabile possono prevedere nella propria politica privacy che la gestione del registro delle attività di trattamento sia affidata al RPD quale parte della sua attività di vigilanza[20]. In tale ambito, il RPD verifica l'avvio di nuovi trattamenti e operazioni di trattamento, effettuando attività di audit per individuare eventuali operazioni poste in essere al di fuori delle procedure stabilite, al fine di garantire il controllo effettivo delle attività da parte del titolare.

Analogamente, sulla base delle informazioni contenute nel RAT, il titolare può affidare al RPD il mantenimento e l'aggiornamento dell'inventario delle attività di trattamento (articolo 31 LOPDGDD) per i

soggetti obbligati[21] o per i titolari e responsabili che, pur non essendovi tenuti, intendano utilizzare volontariamente tale strumento di trasparenza.

In ogni caso, il RPD non dispone di potere decisionale per avviare nuovi trattamenti o nuove operazioni di trattamento. Spetta al titolare dimostrare che il parere del RPD è stato preso in considerazione prima dell'approvazione e dell'avvio delle nuove operazioni o attività.

La politica privacy dell'organizzazione potrebbe coinvolgere concretamente il RPD nei processi di tenuta del registro, prevedendo l'obbligo di richiederne la consulenza e definendo le attività di vigilanza relative al RAT, purché tale coinvolgimento non comporti decisioni sulle finalità e sui mezzi del trattamento o di una specifica operazione di trattamento.

Nota 20. WP243, § 4.5, «Ruolo del RPD nella tenuta dei registri»: spetta al titolare o al responsabile del trattamento, non al RPD, tenere i registri delle operazioni di trattamento. Nulla impedisce tuttavia che il titolare o il responsabile attribuiscano al RPD il compito di tenere il registro sotto la responsabilità del titolare o del responsabile. Tale registro va considerato uno degli strumenti che consentono al RPD di svolgere i compiti di sorveglianza della conformità e di informazione e consulenza nei confronti del titolare o del responsabile.

Nota 21. Articolo 77, comma 1, LOPDGDD.

C. Valutazione d'impatto sulla protezione dei dati (DPIA)

Sulla base di una corretta governance del registro delle attività di trattamento è possibile affrontare la gestione dei rischi per i diritti e le libertà delle persone fisiche. Ove necessario, la consulenza del RPD su tali rischi segnalerà al titolare l'obbligo, la necessità o la raccomandazione di effettuare una valutazione d'impatto sulla protezione dei dati in relazione a un trattamento o a una sua specifica operazione.

La politica privacy può inoltre definire le modalità di coinvolgimento del RPD sin dalla fase di elaborazione concettuale di una nuova attività o operazione di trattamento, nonché gli obiettivi di tale coinvolgimento. Fra questi possono rientrare la consulenza sulla descrizione delle operazioni di trattamento, sul rischio intrinseco, sulla metodologia per la gestione dei rischi o per la DPIA, sulle misure di protezione dei dati fin dalla progettazione e per impostazione predefinita, sulle misure di sicurezza, sull'opportunità di affidare la DPIA all'esterno e sulla necessità di proporre al titolare modifiche alla configurazione iniziale del trattamento o delle operazioni.

Infine, il RPD può assistere il titolare nella valutazione conclusiva della DPIA e, qualora permanga un rischio residuo elevato[22], consigliargli e proporgli di consultare[23] l'autorità di controllo attraverso la consultazione preventiva prevista dall'articolo 36 del GDPR. Quale punto di contatto con l'autorità[24], il RPD può anche richiederne direttamente la consulenza in merito ai rischi delle operazioni di trattamento.

In definitiva, il titolare e il responsabile del trattamento devono coinvolgere il RPD nell'identificazione e valutazione dei rischi, nell'individuazione delle misure di protezione fin dalla progettazione e di minimizzazione, nella proposta dei requisiti di sicurezza dei trattamenti e delle singole operazioni e in ogni altra questione per la quale la sua consulenza possa migliorare la tutela dei diritti e delle libertà delle persone fisiche. Come in ogni caso di disaccordo fra consulenza del RPD e decisione del titolare, occorre documentare la divergenza e le ragioni che hanno indotto il titolare ad assumere una decisione contraria al parere del RPD.

In nessun caso il RPD approva o assume la decisione finale di proseguire un trattamento o di adottare determinate garanzie: tali decisioni spettano al titolare del trattamento, ancorché assistito dalla consulenza del RPD.

Un'ipotesi particolare di consulenza al titolare nell'ambito delle pubbliche amministrazioni riguarda l'elaborazione di progetti normativi. In tale contesto, la consulenza del RPD è fondamentale per individuare misure normative eventualmente non necessarie, sproporzionate o non conformi al diritto di uno Stato membro o al diritto in generale[25]. Il suo coinvolgimento è essenziale affinché le misure legislative rispettino i principi di necessità e proporzionalità, laddove comportino una riduzione dei diritti e delle libertà delle persone fisiche, anche quando non sia inizialmente possibile individuare le operazioni di trattamento cui potranno dar luogo.

Una politica che attribuisca al RPD la responsabilità di effettuare o approvare la DPIA, gestire i rischi per i diritti e le libertà oppure assumere la decisione definitiva sulle misure di protezione dei dati fin dalla progettazione o per impostazione predefinita e sulle misure di sicurezza potrebbe generare un conflitto di interessi, ponendolo nella condizione di dover sorvegliare successivamente decisioni o attività delle quali egli stesso è responsabile.

Nota 22. Guida «Gestione del rischio e valutazione d'impatto nei trattamenti di dati personali»: la consultazione preventiva ha lo scopo di presentare all'autorità di controllo un trattamento conforme al GDPR per il quale sia obbligatorio, o sia stata valutata l'opportunità di, una DPIA, ma che comporti un livello di rischio residuo per i diritti e le libertà delle persone potenzialmente inaccettabile.

Nota 23. L'articolo 39, paragrafo 1, lettera e), del GDPR stabilisce, fra i compiti del RPD, quello di fungere da punto di contatto con l'autorità di controllo per questioni connesse al trattamento, compresa la consultazione preventiva di cui all'articolo 36, ed effettuare, se necessario, consultazioni su qualunque altra questione.

Nota 24. L'articolo 39, paragrafo 1, lettera e), del GDPR include fra i compiti minimi del RPD quello di fungere da punto di contatto con l'autorità di controllo per questioni relative al trattamento, compresa la consultazione preventiva di cui all'articolo 36, e di effettuare, se necessario, consultazioni su qualunque altra questione.

Nota 25. Guida «Orientamenti per lo svolgimento di una valutazione d'impatto sulla protezione dei dati nell'elaborazione normativa».

D. Violazioni della sicurezza dei dati personali

La consulenza del RPD al titolare e al responsabile in materia di rischi per i diritti e le libertà delle persone fisiche deve comprendere anche i rischi che una violazione dei dati personali può comportare per gli interessati, come richiesto dall'articolo 32 del GDPR[26]. La politica privacy può stabilire i meccanismi per assicurare tale consulenza e il reporting al titolare, affinché risulti documentata l'attività consultiva e di vigilanza del RPD in caso di violazione dei dati personali.

La politica privacy può altresì prevedere il coinvolgimento concreto del RPD nei processi di notifica all'autorità di controllo (articolo 33 GDPR) e di comunicazione agli interessati (articolo 34 GDPR), considerando che l'articolo 39 del GDPR include fra i suoi compiti la cooperazione con l'autorità di controllo e la funzione di punto di contatto per le questioni relative ai trattamenti[27], come la notifica di violazioni dei dati personali.

A seguito della consulenza del RPD al titolare o al responsabile in materia di violazioni dei dati, possono essere predisposte note e relazioni tecniche interne sulle misure di protezione fin dalla progettazione e per impostazione predefinita, sulla sicurezza o su qualsiasi altro aspetto connesso alle violazioni verificatesi nell'organizzazione. Tali documenti possono essere approvati o respinti dal titolare, che deve dare evidenza dell'approvazione o del dissenso.

Questa consulenza e vigilanza del RPD nella gestione delle violazioni non deve essere confusa con la responsabilità operativa di gestione dell'incidente, che compete alle unità tecniche e ai responsabili competenti.

Una politica privacy non può delegare al RPD responsabilità e poteri decisionali relativi a una violazione dei dati personali che comportino direttamente o indirettamente la determinazione delle finalità e dei mezzi del trattamento.

Nota 26. Articolo 32, paragrafo 2, del GDPR: nel valutare l'adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento, derivanti in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Nota 27. Articolo 39, paragrafo 1, lettere d) ed e), GDPR: d) cooperare con l'autorità di controllo; e) fungere da punto di contatto con l'autorità di controllo per questioni connesse al trattamento, compresa la consultazione preventiva di cui all'articolo 36, ed effettuare, se necessario, consultazioni su qualunque altra questione.

E. Audit in materia di protezione dei dati

I compiti di consulenza e vigilanza del RPD comprendono la verifica dell'effettiva attuazione delle misure e del loro aggiornamento, ove necessario[28]. Sul piano pratico, ciò si traduce nella segnalazione al titolare dell'esigenza di modificare o aggiornare le misure e nella partecipazione agli audit privacy finalizzati ad assicurare la conformità normativa, attribuendo al RPD capacità di verifica e indagine all'interno dell'organizzazione. La partecipazione del RPD costituisce un elemento essenziale per il rispetto della normativa e l'articolo 39 del GDPR include espressamente fra i suoi compiti la partecipazione agli audit necessari per sorvegliare l'osservanza tanto del GDPR quanto delle politiche privacy del titolare o del responsabile.

Uno dei motivi ricorrenti per i quali il RPD può segnalare al titolare la necessità di modificare un trattamento o una sua operazione, o proporre nuove misure tecniche e organizzative, consiste nel verificarsi di una violazione dei dati personali. In tale circostanza è necessario riesaminare la valutazione iniziale dei rischi e l'efficacia delle misure esistenti oppure la necessità di introdurne ulteriori (misure di protezione fin dalla progettazione, minimizzazione, anonimizzazione, crittografia, sicurezza ecc.) per prevenire o mitigare i rischi connessi alla violazione. A seguito di una violazione e nell'esercizio dei compiti di consulenza e vigilanza sui rischi per i diritti e le libertà delle persone, il RPD può proporre al titolare un audit su un determinato trattamento o operazione, oppure un audit privacy dell'intera organizzazione.

Nota 28. Articolo 24, paragrafo 1, del GDPR: tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare mette in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

VII. Situazioni che richiedono una valutazione specifica dell'indipendenza del RPD

In linea generale, la compatibilità fra le funzioni del RPD e altri incarichi o responsabilità non può essere determinata esclusivamente sulla base della denominazione formale della posizione. Occorre un esame caso per caso, considerando le funzioni effettivamente esercitate, il potere decisionale associato al ruolo e la concreta struttura organizzativa.

Può tuttavia sussistere un conflitto di interessi quando le funzioni aggiuntive consentano al RPD di determinare, approvare o influenzare in misura decisiva le finalità e i mezzi di trattamenti che dovrà successivamente sorvegliare. La mera partecipazione ad attività di consulenza, supporto, coordinamento o verifica non implica necessariamente un conflitto, purché il RPD non assuma la decisione finale, non vigili sulle proprie attività e non riceva istruzioni idonee a comprometterne l'indipendenza. Esistono nondimeno circostanze nelle quali la natura delle funzioni e responsabilità assunte può dare luogo a conflitti di interessi.

In ogni caso, il titolare o il responsabile del trattamento deve valutare e graduare i rischi di conflitto di interessi nelle situazioni potenzialmente incidenti sull'indipendenza del RPD. Ciò vale in generale quando il RPD può decidere, in varia misura, le finalità e i mezzi del trattamento o, pur senza assumerne la decisione, può incidere sull'attuazione o sul dispiegamento del trattamento oltre i compiti propri della funzione. Dopo aver valutato i rischi, occorre individuare misure idonee a mitigarli, come la segregazione funzionale, la validazione indipendente da parte di un terzo o l'astensione regolamentata. La procedura, la valutazione del rischio potenziale e quella del rischio residuo dopo l'applicazione delle misure devono essere adeguatamente documentate.

Questa sezione fornisce orientamenti per identificare possibili rischi di conflitto di interessi nell'esercizio delle attività del RPD, affinché il titolare o il responsabile, secondo i casi, li individui e adotti misure capaci di ridurli o eliminarli. Le posizioni e situazioni esaminate hanno pertanto carattere orientativo e non costituiscono un elenco di incompatibilità automatiche o strutturali: devono essere valutate alla luce dell'efficacia delle misure di mitigazione.

A. Il RPD nelle procedure di affidamento

La partecipazione tempestiva del RPD alle procedure di affidamento è necessaria per individuare requisiti di progettazione e funzionalità che, per impostazione predefinita, siano meno invasive per gli interessati o comportino comunque rischi inferiori per i loro diritti e libertà.

Oltre ai contratti, tuttavia, vi sono altri vincoli giuridici (protocolli, convenzioni, accordi ecc.) che possono implicare trattamenti o operazioni su dati personali e la cui predisposizione richiede il coinvolgimento del RPD, non solo per la verifica delle clausole richieste dall'articolo 28 del GDPR, ma anche per la conformità complessiva alla disciplina sulla protezione dei dati.

L'acquisizione di prodotti o servizi i cui processi coinvolgono dati personali richiede una consulenza tempestiva e adeguata del RPD al titolare, sia per scegliere soluzioni più idonee alla tutela dei diritti e delle libertà delle persone, sia per garantire la minimizzazione nella configurazione.

La consulenza può riguardare i flussi internazionali di dati (capo V del GDPR), il monitoraggio e la revisione del rapporto contrattuale (articolo 28 GDPR), nonché l'obbligo di diligenza nella selezione dei terzi coinvolti nel trattamento. Il titolare e il responsabile dovrebbero pertanto richiedere il parere del RPD prima della

definizione dei requisiti e dell'affidamento dei prodotti e servizi; tale adempimento può essere disciplinato nella politica privacy. Dopo la conclusione del contratto, il RPD fornirà consulenza sullo sviluppo e sulla configurazione predefinita del prodotto o servizio e svolgerà gli audit necessari affinché il titolare possa dimostrare la conformità al GDPR.

In nessun caso spetta al RPD decidere l'acquisto di un prodotto o servizio, assumere decisioni sulla sua configurazione o rappresentare il titolare nelle relative procedure di acquisizione.

Un RPD che lavori nell'ufficio acquisti e rappresenti il titolare nelle procedure di affidamento assumerebbe decisioni sulle gare o sui contratti che possono comportare l'affidamento di trattamenti di dati personali, sia dal lato della stazione appaltante sia da quello dell'affidatario. Qualora il RPD partecipi con potere decisionale alla contrattazione o alla negoziazione dei capitolati, sussiste il rischio di conflitto di interessi, poiché potrebbe finire per sorvegliare le proprie decisioni.

Un RPD che partecipi con il dipartimento ICT alla configurazione predefinita delle piattaforme e alle decisioni sulle informazioni che tali piattaforme raccoglieranno sulle persone fisiche, o sui tempi di conservazione dei log, assumerebbe decisioni di configurazione dei sistemi sulle quali dovrà successivamente vigilare. Ciò contrasterebbe con l'obbligo di indipendenza e obiettività previsto dalla disciplina e determinerebbe un rischio di conflitto di interessi.

B. RPD titolare di altri ruoli e responsabilità nell'organizzazione

L'articolo 38, paragrafo 6, del GDPR[29] consente al RPD di svolgere altri compiti e funzioni. In tal caso, il titolare o il responsabile del trattamento deve garantire che la collocazione gerarchica e le ulteriori responsabilità non generino conflitti di interessi tali da comprometterne l'autonomia tecnica e l'indipendenza funzionale.

I profili che possono rivelare conflitti di interessi sono direttamente connessi all'indipendenza funzionale del RPD. La regola pratica principale è che una posizione che, direttamente o indirettamente, definisce, concorre a definire o approva le finalità e i mezzi del trattamento dei dati personali non è compatibile con la designazione del suo titolare quale RPD.

L'accertamento di un conflitto di interessi richiede una valutazione caso per caso, considerando la specifica struttura organizzativa e tutte le normative applicabili.

Di seguito sono esposti alcuni esempi di posizioni e situazioni che possono frequentemente determinare conflitti di interessi e quindi risultare incompatibili.

1. Posizioni di alta direzione con compiti decisionali operativi sull'utilizzo dei dati

Nelle linee guida WP243, l'EDPB ha indicato che incarichi quali direttore generale, direttore operativo, direttore finanziario, direttore sanitario, responsabile marketing, responsabile delle risorse umane o direttore IT sono, di regola, considerati incompatibili con il ruolo di RPD. Il cumulo della funzione di RPD con ruoli di alta direzione richiede particolare cautela. Anche posizioni meno elevate nella gerarchia possono generare conflitti qualora comportino, direttamente o indirettamente, la determinazione delle finalità e dei mezzi del trattamento.

I responsabili delle tecnologie dell'informazione e della comunicazione (ICT), o di funzioni analoghe, non possono assumere il ruolo di RPD quando le loro competenze comportano decisioni sull'esistenza del trattamento, sulle modalità di trattamento dei dati o sulla configurazione di sistemi, prodotti o servizi che dovrebbero successivamente controllare in qualità di RPD. Il RPD opera come consulente e soggetto di vigilanza interno, non come decisore in materia di trattamenti.

Le posizioni di alta direzione, come quella del responsabile marketing, sono considerate in conflitto con il ruolo del RPD, poiché comportano decisioni sulle finalità e sui mezzi di trattamenti di dati personali per campagne, sviluppo di prodotti, gestione clienti, ricerche di mercato, profilazione ecc.

Il responsabile delle risorse umane è un'altra posizione dirigenziale considerata in conflitto, in quanto implica decisioni sul trattamento dei dati personali dei dipendenti e di altre persone coinvolte nei rapporti di lavoro. La direzione HR gestisce i dati del personale e decide processi e strumenti per il loro trattamento: un RPD coincidente con tale funzione sorveglierebbe le proprie decisioni in una situazione di evidente conflitto. Il problema non riguarda soltanto la direzione HR: anche addetti a livelli inferiori possono essere coinvolti direttamente o indirettamente nelle decisioni sui dati dei lavoratori o sulla scelta e configurazione di piattaforme e sistemi HR.

In generale, possono risultare incompatibili con il ruolo di RPD i responsabili di uffici e unità che decidono sui dati, quali gli uffici anagrafici, le unità che gestiscono le cartelle cliniche, la videosorveglianza, il pagamento di tributi e simili. Ciò può avvenire anche a livelli inferiori dell'alta direzione, se le funzioni comportano la determinazione o l'influenza diretta sulle finalità e sui mezzi dei trattamenti o il coinvolgimento, diretto o indiretto, in tali decisioni. Per esempio, vi rientrano i responsabili di unità che decidono sull'impiego di banche dati particolarmente delicate o di grandi dimensioni nel settore pubblico.

Nota 29. Articolo 38, paragrafo 6, GDPR: «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».

2. Responsabile della sicurezza delle informazioni (CISO/RSI), se decide misure, strumenti o livelli di sicurezza

La figura del RPD deve essere distinta da quella del responsabile della sicurezza delle informazioni (RSI o CISO), disciplinata dal regio decreto spagnolo 43/2021 del 26 gennaio e richiamata nel regio decreto spagnolo 311/2022 del 3 maggio, che disciplina il Sistema nazionale di sicurezza (*Esquema Nacional de Seguridad*). L'RSI può adottare decisioni sui trattamenti di dati per finalità di sicurezza o ricevere istruzioni dirette dal responsabile delle informazioni, mentre il GDPR esige che il RPD non riceva istruzioni dal titolare del trattamento o dal responsabile delle informazioni nell'esercizio delle funzioni.

Il RPD fornisce consulenza al titolare sulle valutazioni d'impatto e su ogni altro aspetto del trattamento, ma è il titolare ad assumere le decisioni definitive sulle finalità, sui mezzi e sulle garanzie necessarie alla tutela dei diritti e delle libertà e alla protezione degli interessi delle persone fisiche. L'RSI garantisce la sicurezza delle informazioni e dei sistemi informativi, mentre il RPD consiglia le misure di sicurezza necessarie a garantire i diritti e le libertà delle persone nel trattamento dei loro dati.

Attribuire al RPD responsabilità dirette in un ambito che deve controllare e nel quale risulterebbe soggetto a istruzioni di altri organi ne impedisce l'indipendenza e genera conflitti di interessi nell'attività di vigilanza.

Eccezionalmente, nelle organizzazioni piccole e con risorse limitate, la designazione della stessa persona quale RPD e RSI potrebbe essere ammissibile, purché siano assicurate e documentate misure organizzative che ne garantiscano l'autonomia, l'indipendenza e l'assenza di conflitti di interessi[30]. Tale situazione deve intendersi transitoria e deve essere risolta non appena possibile. Potrebbe essere il caso, per esempio, di un organismo di nuova costituzione non ancora dotato delle risorse necessarie per designare separatamente entrambe le figure.

Nota 30. Parere giuridico 2018-0170.

3. Responsabile del canale etico e del canale interno di segnalazione[31]

Il responsabile del canale etico o di segnalazione è la persona designata dall'organizzazione obbligata che, in qualità di responsabile del sistema, assume decisioni relative alle informazioni personali trattate. Poiché il RPD deve prestare consulenza e vigilanza sui trattamenti svolti nell'ambito della legge spagnola 2/2023, il cumulo delle funzioni lo collocherebbe in una situazione di evidente conflitto: dovrebbe infatti sorvegliare le decisioni adottate come responsabile del canale etico o del canale di segnalazione.

Anche quando il responsabile del canale interno di protezione del segnalante (*sistema interno de información*) sia un organo collegiale di cui faccia parte il RPD, l'organizzazione deve prevedere meccanismi di astensione nel caso in cui l'esercizio di entrambe le funzioni possa determinare un potenziale conflitto di interessi. La medesima soluzione è richiesta per i canali etici delle organizzazioni.

Nota 31. Legge spagnola 2/2023, del 20 febbraio, che disciplina la protezione delle persone che segnalano violazioni normative e la lotta contro la corruzione.

4. Chief Data Officer / Analisi dei dati / IA / Data Science con potere di definire usi dei dati e modelli

La rapida adozione di modelli di intelligenza artificiale (IA) nelle organizzazioni richiede al RPD nuove competenze che gli consentano di esercitare la funzione fin dalle fasi iniziali di progettazione dei sistemi di IA o di valorizzazione dei dati, nonché nella definizione dei casi d'uso e dei modelli.

Ciò pone nuove sfide nel rapporto fra questi ruoli emergenti e quello del RPD, senza che quest'ultimo possa per questo assumere decisioni sulle finalità o sui mezzi dei sistemi di IA o di qualunque analisi dei dati sulla quale è tenuto a vigilare.

Il RPD non può decidere la selezione dei set di dati o l'utilizzo di meccanismi di IA nei processi dell'organizzazione, né assumere decisioni su finalità secondarie cui destinare dati raccolti originariamente per scopi differenti (*machine learning*, analisi dei dati ecc.). La sua consulenza e vigilanza costituiscono tuttavia fattori chiave per garantire la fiducia degli interessati, in particolare rispetto ai possibili usi secondari dei dati personali.

In generale, il RPD non assume decisioni definitive sulle finalità e sui mezzi dell'IA o sugli impieghi dei dati, ma può e deve assistere il titolare sulla scelta e adeguatezza dei set di dati, sulla presenza di dati eccedenti, sui meccanismi di IA, sugli impieghi secondari e sulle eventuali alternative in grado di ridurre l'impatto sui diritti e sulle libertà delle persone fisiche.

C. Posizioni organizzative potenzialmente compatibili

Le posizioni potenzialmente compatibili con il ruolo del RPD sono quelle che, per loro natura, si concentrano su consulenza, verifica o audit, senza comportare poteri decisionali sulle finalità e sui mezzi del trattamento dei dati personali.

La valutazione del possibile conflitto derivante dal cumulo con altre funzioni deve essere effettuata caso per caso, considerando la struttura organizzativa specifica e tutte le norme applicabili. I conflitti di interessi relativi a tali posizioni possono essere qualificati come effettivi, apparenti o potenziali secondo la terminologia ISO. Nella pratica, sarebbe preferibile disporre di un RPD a tempo pieno e aggiungere altre funzioni solo ove possibile.

1. Consulenza legale / Compliance normativa

L'attività di consulenza legale o compliance è una delle aree di specializzazione più comuni del RPD. È compatibile con tale ruolo purché l'intervento resti circoscritto alla consulenza, all'orientamento e alla vigilanza, senza partecipare all'approvazione o alla determinazione delle finalità e dei mezzi dei trattamenti.

La compatibilità deve essere esaminata sulla base delle responsabilità concretamente assunte. Può insorgere conflitto di interessi quando la persona designata RPD adotti decisioni operative sui trattamenti che debba poi sorvegliare o le sia affidata la rappresentanza o la difesa dell'organizzazione in questioni nelle quali deve mantenere una posizione indipendente come RPD.

Quando al RPD viene chiesto di rappresentare il titolare o il responsabile del trattamento dinanzi agli organi giurisdizionali o in procedimenti per violazioni della disciplina privacy, si determina un conflitto di interessi: egli assume la difesa dell'organizzazione e dei suoi interessi, rendendo difficoltosa la neutralità del proprio ruolo di consulenza e vigilanza.

2. Internal audit / Gestione dei rischi / Qualità

Le funzioni di internal audit e gestione dei rischi sono svolte da figure che valutano e raccomandano, senza, al pari del RPD, assumere decisioni definitive sull'attuazione delle misure, sulle finalità e sui mezzi del trattamento o sulla configurazione di sistemi o dispositivi, come nell'ambito della DPIA. Il titolare e il responsabile del trattamento conservano le rispettive qualifiche e responsabilità, indipendentemente dalla consulenza e dalla vigilanza ricevute in relazione al GDPR.

Quando l'ambito o la portata dell'audit eccede i compiti propri del RPD, l'indipendenza della funzione può risultare compromessa.

Un conflitto sorgerebbe se il RPD partecipasse alla gestione dei rischi finanziari assumendo decisioni sulla capacità economica degli interessati oppure intervenisse in un audit o in una ricerca di mercato che, al fine di realizzare profili di consumo, comporti l'analisi e la selezione di potenziali clienti sulla base di determinati profili.

3. Trasparenza, archiviazione e governo dei dati

Il RPD contribuisce alla trasparenza dei trattamenti di dati personali. A tale scopo, i suoi compiti di vigilanza possono richiedere la raccolta di informazioni per individuare le attività di trattamento e analizzarne e verificarne la conformità. Queste funzioni sono compatibili se il RPD non ha potere decisionale sulle modalità di archiviazione, gestione o utilizzo dei dati: deve potervi accedere esclusivamente per finalità di vigilanza e consulenza, onde accertare il rispetto del GDPR.

Se l'accesso ai dati personali implica decisioni nei processi operativi, come amministrare i dati, attuare misure di sicurezza, modificare il loro ciclo di vita o progettare sistemi di conservazione, il RPD determinerebbe finalità e mezzi del trattamento e opererebbe in conflitto di interessi, dovendo sorvegliare le proprie attività di governo dei dati.

4. Ispezioni di servizio e RPD

L'ispezione di servizio di un'istituzione consiste in un processo di vigilanza e controllo per verificare il corretto svolgimento delle funzioni e il rispetto di norme e procedure. Nella misura in cui l'attività ispettiva comporti decisioni sulle finalità e sui mezzi del trattamento delle informazioni raccolte, la successiva vigilanza da parte del medesimo ispettore in qualità di RPD determinerebbe un conflitto di interessi e potrebbe comprometterne l'imparzialità.

L'adozione di protocolli di astensione in caso di conflitto di interessi potrebbe consentire la compatibilità delle due funzioni.

D. Alcune situazioni suscettibili di compromettere l'indipendenza del RPD o favorire possibili conflitti di interessi

1. Accesso a informazioni sensibili[32] o riservate in qualità di RPD

L'accesso a informazioni sensibili o riservate non costituisce automaticamente un conflitto di interessi. Tuttavia, quando il RPD ricopre anche altri ruoli o funzioni nell'organizzazione, tale accesso può determinarne uno. Potrebbe essere il caso dell'accesso del RPD a informazioni riservate o classificate. La valutazione deve concentrarsi sull'eventuale generazione di un conflitto effettivo, potenziale o apparente a causa del cumulo delle funzioni e sulle misure per gestirlo.

Nota 32. «Informazioni sensibili»: qualunque informazione classificata, relativa al canale di segnalazione, a procedimenti sanzionatori o penali, informazioni riservate, personali, relative al segreto industriale o all'intelligence nazionale o commerciale ecc.

2. Svolgere il ruolo di responsabile del trattamento

Quando un responsabile o sub-responsabile del trattamento agisce contemporaneamente quale RPD, finisce per sorvegliare e prestare consulenza sulle proprie attività di trattamento in qualità di responsabile o sub-responsabile. Ciò determina un evidente conflitto di interessi che può comprometterne l'indipendenza e l'autonomia come RPD.

La situazione può verificarsi quando viene acquistato un prodotto o servizio che include anche l'esercizio delle funzioni di RPD.

Se il medesimo soggetto che fornisce il prodotto o servizio svolge anche la funzione di RPD e sorveglia e fornisce consulenza sulle proprie attività di trattamento in qualità di responsabile o sub-responsabile, tale attività di consulenza e vigilanza risulterebbe priva di valore, potendo configurare un evidente conflitto di interessi.

3. Rappresentanza legale o difesa dell'organizzazione

L'attribuzione al RPD del compito di presentare memorie difensive a tutela dell'organizzazione in procedimenti amministrativi, civili, di lavoro o penali che comportino un trattamento di dati personali è considerata un'ingerenza nelle sue funzioni. Gli richiede infatti di assumere un ruolo estraneo alla missione di consulenza e vigilanza, compromettendone neutralità e imparzialità.

La medesima situazione può verificarsi quando al RPD viene chiesto di rappresentare il titolare o il responsabile dinanzi a un giudice oppure di presentare memorie difensive in procedimenti per violazione della normativa, ammonimenti o procedimenti relativi all'esercizio dei diritti avviati su impulso di un'autorità di controllo in materia di protezione dei dati.

In generale, quando il RPD rappresenta il titolare o il responsabile del trattamento può determinarsi un evidente conflitto, poiché egli non può esercitare pienamente la funzione critica di vigilanza sui trattamenti se deve al contempo difendere altri interessi del titolare.

4. Pluralità di funzioni e insufficienza delle risorse

Sebbene il GDPR consenta al RPD di svolgere altri compiti, essi non devono generare conflitti di interessi. La capacità del RPD di assolvere tutte le funzioni nelle quali è coinvolto è limitata, e la concreta impossibilità di svolgerle o l'insufficienza delle conoscenze necessarie per adottare decisioni in ambiti differenti possono incidere negativamente sui suoi compiti di RPD. Per esempio, quando assume numerose funzioni aggiuntive, specialmente in diversi dipartimenti quali audit, risk management e compliance, aumenta la

probabilità di conflitto non solo per la posizione ricoperta, ma anche per il volume degli incarichi da svolgere.

La molteplicità delle funzioni può portare ad abbandonare, del tutto o in parte, i compiti di RPD oppure a dare priorità alle diverse attività sulla base di interessi propri o di terzi.

Quando il RPD deve assistere contemporaneamente un numero elevato di titolari e responsabili del trattamento, il rischio di conflitto è alto. Esso si accentua quando tale assistenza è prestata a costi anormalmente bassi, che possono indicare l'impossibilità, per l'offerente, di svolgere correttamente i compiti al prezzo proposto e, di conseguenza, l'insufficienza delle risorse economiche necessarie. In queste ipotesi la sostenibilità dell'offerta deve essere adeguatamente giustificata, soprattutto negli affidamenti delle pubbliche amministrazioni.

5. RPD a tempo parziale o condiviso

I RPD a tempo parziale o condivisi fra più organizzazioni possono trovarsi in un conflitto permanente nella ripartizione del tempo e degli sforzi, che indebolisce indipendenza e imparzialità per effetto della posizione ricoperta. Ne possono derivare conflitti nella scelta di quale titolare assistere o sorvegliare prioritariamente e delle modalità della consulenza e vigilanza.

Un unico RPD che presti consulenza e vigilanza a un numero di titolari superiore a quello ragionevolmente gestibile con adeguata disponibilità e reperibilità difficilmente potrà dimostrare l'effettività della consulenza. Inoltre, nell'esercizio della funzione si troverebbe in un chiaro conflitto nel privilegiare un titolare rispetto ad altri.

6. Mancanza d'indipendenza nella gestione

Quando il RPD non può riferire ai massimi vertici, da un lato la sua indipendenza può essere compromessa e, dall'altro, l'alta direzione può non essere pienamente consapevole dei rischi privacy assunti. Ciò avviene quando tra RPD e alta direzione si interpongono soggetti che riferiscono al titolare il contenuto della consulenza e vigilanza del RPD.

Analogamente, quando il RPD riceve istruzioni dal titolare o dal responsabile si trova in una situazione di mancanza di indipendenza che può generare conflitti nell'attività di consulenza e vigilanza, poiché le verifiche tenderebbero a valutare positivamente le disposizioni del titolare anziché garantire i diritti, le libertà e gli interessi delle persone fisiche.

7. Assenza di salvaguardie interne

La mancanza di procedure interne e di politiche privacy approvate che garantiscano l'indipendenza del RPD e prevengano i conflitti al momento della designazione e nel successivo esercizio delle funzioni rivela un problema di governance dell'organizzazione.

Si raccomanda che le organizzazioni individuino le posizioni incompatibili, elaborino regole interne per prevenire i conflitti, forniscano una spiegazione generale e chiara di tali situazioni, verifichino e attestino l'assenza di conflitti al momento della nomina e prevedano salvaguardie nelle disposizioni interne e nei contratti di servizio per evitare ogni tipo di conflitto o incompatibilità.

Come rileva tuttavia la ISO 37009:2025, il conflitto di interessi può manifestarsi in qualsiasi momento dello svolgimento delle attività di un'organizzazione. Anche il RPD non è immune dal rischio. La gestione dei conflitti di interessi non è un formalismo: è la condizione che consente al RPD di consigliare con competenza e sorvegliare con obiettività, presupposti necessari affinché il titolare e il responsabile del trattamento possano dimostrare la conformità.

VIII. Strumenti di tutela del RPD

Nei casi in cui il RPD subisca pressioni o ingerenze, oppure siano in qualsiasi modo violate le garanzie previste dal suo statuto, deve poter disporre di strumenti per richiedere tutela.

L'articolo 38, paragrafo 3, del GDPR vieta espressamente che il RPD sia rimosso o sanzionato per l'adempimento dei propri compiti. L'articolo 36, comma 2, della LOPDGDD prevede una protezione maggiore per il RPD persona fisica inserita nell'organizzazione del titolare o del responsabile, stabilendo che il RPD interno può essere rimosso o sanzionato soltanto in caso di dolo o colpa grave nell'esercizio delle funzioni.

Come illustrato nella sezione V, la Corte di giustizia dell'Unione europea ha interpretato ampiamente la nozione di misura sfavorevole. Alla luce di tale giurisprudenza, le autorità di controllo, tenuto conto del considerando 97 del GDPR, sostengono la necessità che i RPD possano svolgere le proprie funzioni in modo indipendente. La tutela tende quindi a prevenire ogni misura sfavorevole o ritorsiva idonea a condizionare l'indipendenza, quali la sottrazione sostanziale di funzioni, l'eliminazione di risorse indispensabili, l'isolamento gerarchico o il blocco della progressione professionale.

Strumenti interni

1. Reporting diretto al vertice gerarchico

In presenza di ostruzioni o ingerenze, il RPD deve poter esercitare la facoltà, garantita dal GDPR, di rivolgersi direttamente all'alta direzione (consiglio di amministrazione, direzione generale o sottosegretariato), senza passare attraverso intermediari o filtri.

2. Canale interno di segnalazione e canale etico

Il RPD deve avere accesso al sistema interno d'informazione tramite il canale di segnalazione dell'organizzazione (disciplinato in Spagna dalla legge 2/2023, del 20 febbraio, sulla protezione dei segnalanti e la lotta alla corruzione) per segnalare formalmente pressioni, ritorsioni o conflitti di interessi che ne compromettano o possano comprometterne l'indipendenza.

3. Documentazione e tracciabilità della mancata tutela o delle divergenze

Ai sensi dell'articolo 36, comma 4, della LOPDGDD, quando il RPD rileva una violazione rilevante o una grave insufficienza di risorse e/o garanzie, deve documentarla formalmente e comunicarla immediatamente agli organi di amministrazione.

A. Consultazione o reclamo dinanzi all'autorità di controllo

1. Consultazione dell'autorità di controllo

Il RPD può rivolgere consultazioni e comunicare dubbi o situazioni che incidano sull'adempimento dei propri compiti e del GDPR. Beneficia in ogni caso del dovere di segreto e riservatezza che vincola l'operato dell'autorità di controllo.

2. Avvio di un procedimento d'indagine o sanzionatorio

L'inosservanza, da parte del titolare o del responsabile del trattamento, degli obblighi relativi alla posizione, alle risorse e all'indipendenza del RPD (articoli 37–39 del GDPR) costituisce una violazione della legge.

L'autorità di controllo può disporre accertamenti preliminari o avviare un procedimento sanzionatorio per l'adozione, ove necessario, delle misure correttive o delle sanzioni amministrative pecuniarie previste.

B. Tutela giurisdizionale

Giurisdizione del lavoro o amministrativa

In caso di licenziamento, rimozione dall'incarico, sanzione o modifica sostanziale delle condizioni adottati quale ritorsione per l'esercizio indipendente delle funzioni, il RPD può adire gli organi giurisdizionali per chiedere l'invalidazione della misura e il ripristino delle proprie condizioni e dell'indipendenza.

In caso di rapporto di lavoro subordinato, può rivolgersi alla giurisdizione del lavoro; nel caso dei dipendenti pubblici, alla giurisdizione amministrativa o del lavoro, secondo le regole applicabili.

IX. Conclusione

L'effettività della figura del RPD richiede che la designazione, l'integrazione nell'organizzazione e le condizioni di esercizio dei compiti siano orientate al medesimo obiettivo: garantire una consulenza specialistica e una vigilanza indipendente che contribuiscano all'osservanza della normativa sulla protezione dei dati e consentano di dimostrarla. Le garanzie devono essere mantenute per l'intera durata dell'incarico e applicarsi anche alle decisioni che incidono sulla permanenza o sulla cessazione.

La designazione del RPD non deve ridursi a un adempimento formale. Si raccomanda di documentarne espressamente la nomina, le funzioni, la collocazione organizzativa, le risorse assegnate e i canali di accesso ai massimi vertici. Tale definizione agevola l'effettiva integrazione nella governance e previene divergenze sull'ambito di competenza e sulle condizioni di esercizio delle funzioni. La designazione di un organo collegiale consente di adattare la figura del RPD alle caratteristiche dell'organizzazione e garantisce la continuità della funzione e, in ultima analisi, delle risorse a essa destinate.

La carenza di risorse economiche incide direttamente sull'indipendenza del RPD. Da un lato, la consulenza e la vigilanza potrebbero essere condizionate al raggiungimento di determinati obiettivi economici dell'ente presso cui opera; dall'altro, potrebbe essergli impedito di svolgere le funzioni. Quest'ultima situazione si verifica quando si intende fornire il servizio di RPD a un numero sproporzionato di titolari e responsabili oppure quando il compenso pattuito è irrisorio o manifestamente insufficiente per assicurare un servizio effettivo, situazione particolarmente critica per i titolari appartenenti alle pubbliche amministrazioni.

Affinché il RPD possa consigliare con competenza e sorvegliare con obiettività, deve godere di uno status che gli consenta di agire liberamente. Il titolare o il responsabile del trattamento devono garantirne il coinvolgimento adeguato e tempestivo nelle questioni relative alla protezione dei dati, l'accesso alle informazioni necessarie e la disponibilità di risorse materiali e umane, tempo, formazione continua e supporto organizzativo sufficienti. Il RPD non deve inoltre ricevere istruzioni sul contenuto della consulenza, delle indagini o delle attività di vigilanza.

Il reporting diretto ai massimi vertici costituisce una garanzia sostanziale di indipendenza. L'organizzazione deve predisporre canali effettivi affinché il RPD comunichi le raccomandazioni, segnali rischi e violazioni rilevanti e rappresenti le esigenze connesse all'esercizio dei compiti. L'interlocuzione deve consentire alla direzione di conoscere e considerare la consulenza del RPD prima di adottare decisioni e di ricevere tempestivamente le comunicazioni che richiedono un intervento immediato.

I meccanismi di reporting e rendicontazione devono essere proporzionati alla natura, alle dimensioni, alla complessità e al rischio dei trattamenti. Il GDPR non impone un modello uniforme di relazione né un obbligo generale di redigere un rapporto annuale. Le relazioni periodiche rappresentano una buona prassi, particolarmente utile nelle organizzazioni complesse, che può essere integrata con verbali, comunicazioni documentate, registri delle raccomandazioni o rapporti specifici. È importante poter dimostrare l'effettivo coinvolgimento del RPD e l'adeguata considerazione dei suoi pareri.

La documentazione della consulenza e della vigilanza agevola la tracciabilità delle decisioni. Quando l'organizzazione si discosta dalle raccomandazioni del RPD, è opportuno documentarne le ragioni. Tale prassi rafforza la responsabilizzazione senza modificare il carattere non vincolante delle raccomandazioni e senza trasferire al RPD la responsabilità delle decisioni sui trattamenti.

Il RPD non può in alcun caso ricoprire nell'organizzazione un incarico che lo porti a determinare le finalità e i mezzi del trattamento dei dati personali. Tale limite non impedisce che, nell'esercizio dei compiti consultivi e di vigilanza, partecipi all'analisi di finalità e mezzi e formuli raccomandazioni circa la conformità al GDPR o

proponga alternative idonee a perseguire le finalità legittime del titolare con minore impatto sui diritti e sulle libertà delle persone. La decisione definitiva spetta sempre al titolare.

Le posizioni e situazioni suscettibili di generare conflitti di interessi non costituiscono un elenco chiuso. Le organizzazioni devono valutarle in funzione dell'attività, della struttura, della ripartizione delle competenze e dei rapporti fra le persone coinvolte, tenendo conto di finalità, contesto, portata e natura dei trattamenti. La valutazione deve essere svolta prima della nomina e ripetuta nel tempo, poiché i conflitti possono insorgere durante l'esercizio dei compiti. Il cumulo di funzioni, l'esternalizzazione dei servizi e le relazioni con titolari o responsabili del trattamento devono essere esaminati verificando se compromettano l'obiettività del RPD o lo portino a sorvegliare proprie decisioni o attività.

È essenziale disporre di una politica organizzativa per la gestione dei conflitti di interessi, con garanzie chiare e documentazione coerente. Si raccomanda di individuare gli incarichi incompatibili, stabilire procedure per comunicare e valutare situazioni sopravvenute, definire meccanismi di astensione e ricusazione e inserire garanzie nelle regole interne e nelle condizioni contrattuali. Tali misure devono essere note all'organizzazione e sottoposte a verifica di efficacia.

La protezione dell'indipendenza del RPD comprende sia il divieto di rimozione o sanzione per l'esercizio dei compiti, sia la tutela contro le ritorsioni connesse alla consulenza o alla vigilanza. Tale garanzia non equivale all'inamovibilità assoluta. Quando il RPD è una persona fisica inserita nell'organizzazione, occorre considerare la protezione rafforzata prevista dall'articolo 36, comma 2, della LOPDGDD.

Le decisioni relative a permanenza, funzioni, risorse o posizione istituzionale devono essere esaminate per i loro effetti sostanziali. Una significativa riduzione dei mezzi, la perdita dell'accesso diretto ai vertici o la sottrazione di competenze essenziali possono comprometterne l'indipendenza anche in assenza di cessazione formale. È pertanto raccomandabile acquisire preventivamente il parere del RPD, valutare l'impatto delle misure e documentarne le motivazioni.

La designazione effettiva, la comunicazione diretta con i vertici, la disponibilità di risorse sufficienti, la prevenzione dei conflitti di interessi e le garanzie contro le ritorsioni devono essere concepite come un sistema unitario. La loro finalità è consentire al RPD di consigliare con competenza, sorvegliare con obiettività e contribuire a una cultura organizzativa della protezione dei dati. Il sostegno istituzionale alle sue funzioni favorisce conformità e rendicontazione, preservando le responsabilità proprie del titolare e del responsabile del trattamento e proteggendo diritti, libertà e interessi delle persone fisiche.

In conclusione, il documento non intende imporre un modello organizzativo unico né creare nuovi obblighi giuridici, ma agevolare l'interpretazione e l'applicazione pratica delle garanzie previste dall'ordinamento, rafforzare l'indipendenza funzionale del RPD e promuoverne l'adeguata integrazione nella governance delle organizzazioni, senza sostituire la valutazione giuridica e organizzativa che deve essere compiuta in ciascuna fattispecie.

X. Riferimenti

A. Agenzia spagnola per la protezione dei dati (AEPD)

- AEPD — Piano strategico 2025–2030, presentato il 3 luglio 2025.
- AEPD — Piano d'azione 2026.
- AEPD — Raccomandazioni per rafforzare il rispetto della normativa sulla protezione dei dati nell'Amministrazione generale dello Stato, 14 luglio 2026.
- AEPD — L'AEPD promuove un modello comune di conformità nel settore pubblico, con raccomandazioni e prossime iniziative (comunicato stampa, 14 luglio 2026).
- AEPD — Risultati dell'azione europea che ha esaminato la designazione e la posizione dei responsabili della protezione dei dati (comunicato stampa, 2024).
- AEPD — Istruzione n. 1/2021, del 2 novembre, recante orientamenti sull'attività consultiva dell'Agenzia (BOE del 5 novembre 2021).
- AEPD — Parere giuridico n. 0170/2018, del 12 novembre 2018, sulla compatibilità fra RPD e responsabile della sicurezza nell'ambito dello *Esquema Nacional de Seguridad*.
- AEPD — Parere giuridico n. 0167/2018, sulla separazione fra RPD e responsabile della sicurezza nell'ambito dello *Esquema Nacional de Seguridad*.
- AEPD — Parere giuridico n. 0037/2020, sulla designazione di un medesimo RPD per più titolari o responsabili del trattamento e sui requisiti della nomina.
- AEPD — Parere giuridico n. 0048/2021, su una politica di sicurezza delle informazioni e sulla posizione del RPD nella struttura di sicurezza.
- AEPD — Parere giuridico n. 0038/2023 (rif. 0096/2022), sulla posizione giuridica e sulle funzioni del RPD.
- AEPD — Parere giuridico n. 0034/2023.
- AEPD — Provvedimento nel procedimento sanzionatorio PS/00345/2022 (EXP202201681), del 19 luglio 2023, sulla designazione del segretario di un ordine professionale quale RPD, confermato dalla sentenza dell'Audiencia Nacional n. 139/2026.
- AEPD — Provvedimento del 14 giugno 2024 sul ricorso amministrativo contro la decisione nel procedimento sanzionatorio PS/00382/2023 (EXP202211394), relativo al conflitto di interessi del RPD che presenta memorie difensive in nome del titolare.
- AEPD — Provvedimento nel procedimento sanzionatorio PS/00548/2024 (EXP202316729), del 5 marzo 2026, sull'incompatibilità tra le funzioni di RPD e di responsabile del sistema interno di segnalazione.
- AEPD — Schema di certificazione dei responsabili della protezione dei dati (*Esquema AEPD-DPD*), versione 1.4, 23 dicembre 2019.
- AEPD — *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales* [Gestione dei rischi e valutazione d'impatto nei trattamenti di dati personali], giugno 2021.
- AEPD — *Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo* [Orientamenti per la valutazione d'impatto sulla protezione dei dati nell'elaborazione normativa].
- AEPD — *Protección de datos desde el diseño en los contratos de la Administración Pública* [Protezione dei dati fin dalla progettazione nei contratti della pubblica amministrazione] (blog).

- Korff, D. e Georges, M. (progetto T4DATA) — *El manual del DPD* [Manuale del RPD] (2019), edizione spagnola pubblicata dall'AEPD.

B. Comitato europeo per la protezione dei dati e Garante europeo della protezione dei dati

- Gruppo di lavoro Articolo 29 / EDPB — Linee guida sui responsabili della protezione dei dati (WP243 rev.01), adottate il 13 dicembre 2016 e riviste il 5 aprile 2017, recepite dall'EDPB il 25 maggio 2018.
- EDPB — *2023 Coordinated Enforcement Action – Designation and Position of Data Protection Officers* [Azione coordinata di enforcement 2023 — Designazione e posizione dei RPD]. Relazione adottata il 16 gennaio 2024.
- EDPB — Linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del GDPR, versione 2.0, adottate il 28 marzo 2023.
- EDPS — *Supervisory Guidance – Role of the Data Protection Officers in EU institutions, bodies, offices and agencies*, adottata il 18 dicembre 2025 (versione 1.1 del 5 febbraio 2026).
- EDPS — Decisione 01/2026 del Garante europeo della protezione dei dati, del 16 gennaio 2026, sulle disposizioni attuative del requisito del consenso preventivo dell'EDPS per la rimozione dei RPD (GUUE L 2026/199, 29 gennaio 2026).
- EDPS — *Position Paper on the role of Data Protection Officers of the EU institutions and bodies*, 30 settembre 2018.

C. Autorità regionali spagnole

- CTPDA — *Modelo de instrucción interna para fortalecer el papel del Delegado de Protección de Datos en las entidades del sector público andaluz* [Modello di istruzione interna per rafforzare il ruolo del RPD negli enti del settore pubblico andaluso], febbraio 2025.
- CTPDA — Provvedimento del 16 giugno 2026 che approva il Piano di controllo e ispezione sulla protezione dei dati nel settore pubblico andaluso 2026–2027 (BOJA n. 118 del 22 giugno 2026).
- APDCAT — Parere CNS 17/2024, sulle funzioni del RPD.
- APDCAT — Parere CNS 29/2022.

D. Autorità di controllo di altri Stati

- CNIL — *Le rapport d'activité du DPO : piloter la conformité et valoriser ses actions* [Relazione di attività del DPO: governare la conformità e valorizzare gli interventi] (guida e modello di relazione, 27 aprile 2026).
- CNIL — *Guide pratique RGPD – Délégués à la protection des données* [Guida pratica GDPR — Responsabili della protezione dei dati] (2022), con modello di lettera di incarico.
- CNIL — *Délégué à la protection des données: identifier et gérer les conflits d'intérêts liés à la fonction de DPO* [Individuare e gestire i conflitti di interessi connessi alla funzione di DPO], 10 agosto 2026.
- Autorité de protection des données (Belgio) — *Permettre au délégué à la protection des données d'exercer ses missions en toute indépendance* [Consentire al RPD di svolgere i compiti in piena indipendenza] (aggiornato il 24 gennaio 2024).
- Autorité de protection des données (Belgio) — *Décision quant au fond* n. 18/2020 del 28 aprile 2020 (conflitto di interessi del RPD).

- Autorité de protection des données (Belgio) — Raccomandazione n. 04/2017, del 24 maggio 2017, sulla designazione di un RPD e l'ammissibilità del cumulo con altre funzioni.
- Garante per la protezione dei dati personali (Italia) — *Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico* (provvedimento 29 aprile 2021, n. 186; Gazzetta Ufficiale n. 132 del 4 giugno 2021).
- Autoriteit Persoonsgegevens (Paesi Bassi) — *Positionering van de FG. Uitgangspunten: rollen, processen en verantwoordelijkheden* [Collocazione del RPD: principi di ruoli, processi e responsabilità] (giugno 2021).
- Data Protection Commission (Irlanda) — *Guidance on appropriate qualifications for Data Protection Officers* [Orientamenti sulle qualifiche adeguate per i RPD].
- Data Protection Commission (Irlanda) — Decisione IN-18-12-01, *Department of Employment Affairs and Social Protection*, 10 maggio 2021 (coinvolgimento adeguato del RPD e assenza di istruzioni).
- Ufficio del Difensore per la protezione dei dati (Finlandia) — *Designating a data protection officer* [Designazione di un RPD].
- Datatilsynet (Danimarca) — *Vejledning om databeskyttelsesrådgivere* [Orientamenti sui RPD] (dicembre 2017).
- Integritetsskyddsmyndigheten (Svezia) — *IMY klar med fördjupade granskningar av dataskyddsombudens roll* [Completate le verifiche approfondite sul ruolo dei RPD] (2024; decisioni di vigilanza sul ruolo e sulla posizione dei RPD nell'azione coordinata europea).
- Commission nationale pour la protection des données (Lussemburgo) — Deliberazione n. 18FR/2021 del 31 maggio 2021 e altre decisioni della campagna di audit tematici sulla funzione del RPD (2021).
- Datatilsynet (Norvegia) — *Sanctions imposed on Telenor ASA for lack in the organisation of the data protection officer and lack of internal control* [Sanzioni a Telenor ASA per carenze organizzative relative al RPD e insufficienze del controllo interno] (decisione 10 marzo 2025).

E. Associazioni professionali, norme tecniche e altri riferimenti

- ISO — ISO 37009:2025, *Conflict of interest in organizations — Guidance* [Conflitti di interessi nelle organizzazioni — Linee guida].
- BvD — *Berufsverband der Datenschutzbeauftragten Deutschlands*, *Positionspapier Aufwandsabschätzungen DSB* [Documento di posizione sulla stima dell'impegno richiesto ai RPD] (aprile 2020).
- ISMS Forum — Data Privacy Institute, *El Libro Blanco del DPO* [Libro bianco del DPO], II edizione (febbraio 2025).
- CEDPO — Confederation of European Data Protection Organisations, *Minimum qualifications for Data Protection Officers* [Qualifiche minime dei RPD] (30 maggio 2016).
- CEDPO — Confederation of European Data Protection Organisations, *Follow-up letter on the WP29 Guidelines on Data Protection Officers* [Lettera di follow-up sulle linee guida del WP29 sui RPD] (15 febbraio 2017).
- ENISA — *Mapping NIS2 obligations with ECSF role profiles* [Mappatura degli obblighi NIS2 rispetto ai profili professionali ECSF] (giugno 2025).
- IAPP — *The most iconic DPA decisions on DPOs and what you should take from them* [Le decisioni più emblematiche delle autorità di controllo sui DPO e le indicazioni da trarne] (2023).
- AEC — Club del DPD, *Conflictos de interés del DPD* [Conflitti di interessi del RPD] (I approfondimento esclusivo del Club DPD, 2023; materiale divulgativo).

F. Giurisprudenza

- Corte di giustizia dell'Unione europea, sentenza 22 giugno 2022, *Leistritz*, C-534/20, ECLI:EU:C:2022:495.
- Corte di giustizia dell'Unione europea, sentenza 9 febbraio 2023, *X-FAB Dresden*, C-453/21, ECLI:EU:C:2023:79.
- Corte di giustizia dell'Unione europea, sentenza 9 febbraio 2023, *KISA*, C-560/21, ECLI:EU:C:2023:81.
- Tribunal Supremo [Spagna], Sezione lavoro (*Sala de lo Social*), sentenza 22 settembre 2026, ricorso n. 384/2025.
- Audiencia Nacional [Spagna], Sezione amministrativa (*Sala de lo Contencioso-Administrativo*), Sezione I, sentenza n. 139/2026 del 18 marzo 2026, ricorso n. 894/2023.
- Tribunal Superior de Justicia de Madrid [Spagna], Sezione lavoro (*Sala de lo Social*), sentenza del 2026, STSJ M 7356/2026, ECLI:ES:TSJM:2026:7356, e sentenza n. 910/2021 del 29 dicembre 2021, ricorso n. 476/2021 [V].