Associazione Data Protection Officer
Sede Legale: P.le Principessa Clotilde, 6 – 20121 Milano (MI)
Sede Operativa: Via Brianza, 65 – 22063 Cantù (CO)
info@assodpo.it - www.assodpo.it
C.F. 97656960156
P.IVA 08258580961 (solo per attività commerciale)

DPO e Settore Pubblico

Il Garante per la protezione dei dati personali (di seguito GPDP) con il "**Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD|DPO) in ambito pubblico**" pubblicato a maggio 2021 ha finalmente fatto chiarezza su una serie di criticità che si erano rilevate nell'applicazione del GDPR in tema di designazione, posizione e compiti dell'RPD | DPO.

Il documento di 36 pagine è una sorta di raccolta di precedenti interventi del GDPD a seguito delle istanze pervenutele in questi 3 anni di applicazione della norma.

Il documento nell'introduzione richiama le Pubbliche Amministrazioni a non pensare che la funzione del RPD | DPO sia "*talvolta vissuto come un mero adempimento formale, senza comprendere adeguatamente l'importanza della figura in questione nel supporto e nella vigilanza sulla correttezza dei trattamenti di dati personali effettuati dal titolare*".

Ma andiamo con ordine e scorriamo sinteticamente i punti analizzati nel documento.

Sommario

Associazione Data Protection Officer
Sede Legale: P.le Principessa Clotilde, 6 – 20121 Milano (MI)
Sede Operativa: Via Brianza, 65 – 22063 Cantù (CO)
info@assodpo.it - www.assodpo.it
C.F. 97656960156
P.IVA 08258580961 (solo per attività commerciale)

1. RPD | DPO quale punto di contatto

Il GDPD ribadisce con forza, in più punti del documento, l'indipendenza e autonomia del RPD|DPO, definito dallo stesso "facilitatore", in quanto deve facilitare l'accesso, da parte dei funzionari dell'Autorità ai documenti e alle informazioni necessarie.

Durante le attività di ispezione del GDPD e/o degli uomini del Nucleo Speciale Privacy della GdF, nelle richieste di parere, nelle audizioni il RPD | DPO deve essere "**tempestivamente e adeguatamente**" coinvolto in tutte le questioni riguardanti la protezione dei dati.

Proprio per questa sinergia, già individuata dal GDPR, fra RPD | DPO e GDPD, quest'ultimo invierà in sede di istruttoria preliminare, le richieste di informazioni anche al RPD|DPO, pur rimanendo l'onere di fornire riscontro (e la conseguente responsabilità dell'eventuale inadempimento) in capo al titolare/responsabile.

Il Garante a tal proposito definisce **essenziale la comunicazione tempestiva all'Autorità dei dati esatti di contatto del RPD | DPO** e il suo **aggiornamento**, anche per evitare l'inoltro di comunicazioni a soggetti che non sono (o non sono più) RPD|DPO.

2. Obbligo di designazione RPD | DPO nella PA

Fermo restando l'obbligo di nomina per tutte le PA, il documento sottolinea l'importanza – *fortemente raccomanda* – la nomina del RPD | DPO per quei **soggetti privati che esercitano compiti di interesse pubblico** (es. concessionarie di pubblici servizi con trattamenti GPS – call center ecc.) e **per le strutture sanitarie private e RSA**.

Nel documento si pone l'attenzione anche della specifica della "*vacatio*" fra la conclusione di un incarico RPD | DPO e la nomina del successivo, il ruolo non può essere lasciato scoperto e la P.A. è comunque tenuta ad individuare temporaneamente, al proprio interno, un dirigente o un funzionario da designare interinalmente nel ruolo; con i relativi obblighi di notifica al GDPD.

A tal proposito c'è ancora molta strada da fare; basti pensare che, come emerso in un recente evento CLUSIT, il GDPD ha informato che almeno 1/8 tra i comuni italiani non ha notificato la nomina obbligatoria dell' RPD | DPO.

3. DPO cumulativo

Il documento non aggiunge nulla di nuovo all'art. 37.3 del GDPR, ribadisce che Titolari del trattamento con **strutture organizzative e dimensioni limitate in termini di risorse economiche** (es. istituti scolastici o piccoli enti territoriali) **potrebbero avvalersi di un DPO in comune**, purché sia garantito l'efficace svolgimento dei propri compiti.
L'Autorità suggerisce in tal caso:

- **La costituzione di un gruppo di collaboratori a supporto del RPD | DPO** designato in comune
- Di definire preventivamente la **percentuale del tempo lavorativo** destinata a ciascun Titolare del trattamento
- Di verificare eventuali **conflitti d'interesse**
- Accertarsi che la comunicazione al GDPD sia effettuata per **ciascun ente pubblico**

Si ricorda altresì che in caso di Unione di comuni ciascun comune è tenuto ad effettuare notifica al GDPD e inserire nelle informative i dati di contatto del RPD|DPO.

4. Qualità professionali e possesso di titoli

Il GDPD segnala che nei bandi pubblici analizzati sono generalmente richiesti 3 requisiti al candidato RPD | DPO esterno:

- Laurea in giurisprudenza

- Iscrizione ad albo professionale (avvocati)
- Possesso di particolari certificazioni (UNI 11697)

Questi requisiti non sono stabiliti dal GDPR e il loro possesso, si pensi ad un avvocato che non si è mai occupato di protezione dei dati personali, non sono sinonimo di competenze assicurate; **la valutazione delle competenze andrà sempre effettuata nel concreto dal titolare del trattamento.**

Il GDPD suggerisce di verificare la conoscenza di norme e prassi attraverso:

- Conoscenza approfondita del GDPR, della norma nazionale e delle prassi operative del GDPD
- Documentata esperienza professionale e/o formazione specialistica
- Certificazioni volontarie acquisite sulla base della norma tecnica UNI 11697, quale elemento di valutazione e non abilitazione
- Curriculum vitae dettagliato

5. RPD | DPO esterno

Relativamente alla nomina di RPD | DPO esterni il GDPD lamenta che nel corso delle istruttorie siano emersi casi di non allineamento fra atti, formule ambigue scarsa trasparenza delle nomine, **numeri eccessivi di incarichi acquisiti in capo alla medesima società**, **tempi d'incarico e risorse inadeguate**.

Gli atti di nomina non risultano sempre pienamente allineati tra loro, per cui le indicazioni in ciascuno contenute risultano non univoche. Ad esempio, l'offerta di servizio emessa dalla Società di servizio, indicante la persona fisica che si occuperà di svolgere l'attività di RPD|DPO, diviene contratto di servizio, mentre l'ente con decreto del Sindaco nomina la persona fisica, generando confusione sulle reali responsabilità in capo a ciascun soggetto.

Situazione complicata poi dal fatto che spesso la società di servizio è o viene nominata responsabile del trattamento ai sensi dell'art. 28 GDPR (come, ad esempio, in riferimento alla valutazione d'impatto sulla protezione dei dati |DPIA) o specifici compiti quali, ad esempio, la fornitura di piattaforme tecnologiche o specifiche funzionalità (registro delle attività di trattamento, erogazione di eventi formativi, predisposizione di informative, ecc.).

Il GDPD richiede che vi sia coerenza fra i diversi documenti di assegnazione dell'incarico, che la designazione sia parte integrante dell'apposito contratto di servizio, che sia individuata, in maniera inequivocabile, la persona del RPD|DPO, e che risultino indicate le motivazioni che hanno indotto l'ente a individuare, nella persona fisica selezionata, il proprio RPD|DPO, al fine di consentire la verifica del rispetto dei requisiti.

6. RPD | DPO con numerosi incarichi e attività presso la PA

Altra criticità individuata dagli accertamenti ispettivi condotti è l'esistenza di **società che svolgono incarichi di RPD | DPO per conto di numerosi soggetti pubblici (nell'ordine delle centinaia), spesso anche variamente dislocati sull'intero territorio nazionale**.

Oltre all'incarico di RPD|DPO, è emerso **che tali società svolgono anche altri incarichi** che pur non essendo, in generale, incompatibili con il ruolo di RPD | DPO (ad esempio, quello di referente nell'ambito della sicurezza del lavoro) **potrebbero comunque rendere difficile lo svolgimento di tutti i compiti affidati**, soprattutto quando queste società operano con risorse non adeguate indicando i medesimi collaboratori quali referenti, incidendo anche sulla credibilità della qualità del lavoro svolto come RPD|DPO.

Tutto questo pone un tema di adeguatezza ed efficacia del ruolo del RPD | DPO nello svolgimento dei compiti previsti dall'art. 39 GDPR.

L'ente dovrebbe quindi verificare:

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

Inoltre, **ciascuna amministrazione dovrebbe valutare l'opportunità di individuare, al proprio interno, una figura di riferimento per il RPD | DPO esterno**, con il quale quest'ultimo possa interloquire con costanza.

7. Contratto esterno RPD | DPO: referente della persona giuridica anche a partita IVA

Il GDPD fa chiarezza anche sulla **possibilità**, prima messa in dubbio da qualche TAR, **che la persona giuridica candidata ad assumere l'incarico di RPD | DPO per conto di una PA possa avvalersi di un referente persona fisica che non sia un dipendente della società medesima**, e quindi sia esterno al suo organico; ritenendo che il rapporto di "appartenenza" non debba essere letto in senso giuridico.

Occorre però, in massima trasparenza, dichiarare il tipo di rapporto contrattuale e verificare i requisiti nonché la non numerosità di incarichi ricoperti.

8. Durata dell'incarico

Il **GDPD** indica, in linea di massima, quale **periodo congruo per la durata dell'incarico i tre anni**, al fine di dare al RPD | DPO il tempo necessario per poter conoscere adeguatamente l'organizzazione dell'ente e attuare le misure necessarie a garanzia dei diritti degli interessati.

Il documento pone anche l'attenzione a quanto sostenuto dall'autorità anticorruzione ai fini di rispetto della disciplina in materia di contratti pubblici, sulla necessità che l'affidamento dei contratti aventi ad oggetto il servizio di protezione dei dati personali di importo inferiore alle soglie comunitarie debba avvenire nel rispetto del principio di rotazione.

9. Remunerazione del RPD | DPO

Il GDPD ritiene che **l'eccessivo abbassamento della remunerazione** (si sono rilevati anche incarichi gratis o per poche centinaia di €.) **per la fornitura del servizio di RPD | DPO abbia un duplice effetto negativo**:

- Consentire l'aggiudicazione in favore di candidati che non abbiano una formazione specifica idonea;
- Quello di spingere i soggetti affidatari, per conseguire una remunerazione adeguata, ad accumulare un elevato numero di incarichi, con la conseguenza di non riuscire ad offrire un servizio efficace a ciascuno dei propri clienti.

A tal proposito si suggerisce di non basare le scelte in sede di bando dando uno sproporzionato peso all'elemento prezzo, ma anche ad aspetti di carattere qualitativo delle offerte.

10. Pubblicazione e comunicazione al GDPD

Il GDPD ribadisce e sottolinea l'importanza di pubblicare i dati di contatto del RPD|DPO, nello specifico sulla home page del sito web del Titolare del trattamento, e comunicare i dati di contatto al GDPD stesso.

Si suggerisce inoltre di rendere disponibili, sia nei confronti del pubblico che dell'Autorità, una casella "istituzionale" ad hoc attribuita specificamente al solo RPD | DPO, evitando l'utilizzo di caselle che siano direttamente espressione del Titolare del trattamento (ad esempio, perché richiamano l'"amministrazione", la "segreteria" o il "protocollo").

Invero, perché sia effettivamente indipendente nell'esercizio delle sue funzioni (come richiesto dal cons. 97 del Regolamento), sarebbe opportuno che il RPD | DPO venisse contattato attraverso canali che riconducano direttamente a lui, senza l'intermediazione di uffici facenti capo al Titolare del trattamento.

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

11. Coinvolgimento del Titolare del trattamento | frequenza incontri

Il GDPD lamenta inoltre **la prassi di instaurare contatti, solo saltuari, pratica che vanifica il senso della presenza del RPD | DPO** e, con esso, **l'approccio di privacy by design e by default** promosso dal GDPR; facendo emergere un tema di inadeguatezza dei compiti previsti dall'art. 39 GDPR.

Il GDPD ritiene critica la situazione in cui ci siano gli RPD | DPO poco propositivi e i Titolari del trattamento portati a considerare la figura del RPD | DPO quale mero adempimento formale.

Tale atteggiamento può essere imputabile a entrambe le parti: al RPD|DPO, "*in quanto spesso portato a non proporre adeguatamente al titolare le attività necessarie per conformare i trattamenti alla disciplina in materia di protezione dei dati personali*; alla PA*, per la tendenza a considerare la nomina del RPD solo come un adempimento formale, non riconoscendo e tantomeno valorizzando i compiti e le potenzialità di questa figura*".

Al fine di rendere effettivo il coinvolgimento del RPD | DPO il GDPD suggerisce alcune **buone pratiche, anche da formalizzare contrattualmente**:

A. L'individuazione, all'interno dell'amministrazione, di una **figura**, adeguata per posizione e competenze, **che funga da punto di riferimento per il RPD|DPO**, con il quale quest'ultimo possa interloquire costantemente;
B. La condivisione di **un'agenda con incontri periodici**;
C. La **proposta**, da parte del RPD | DPO al Titolare del trattamento, **di attività di miglioramento continuo** (formazione, informazione, revisione documentale, registro del trattamento, verifica misure di tecniche e organizzative, policy di data breach, rendicontazione attività svolte).

Il GDPD suggerisce altresì di non assegnare al RPD | DPO compiti che spettano al Titolare del trattamento e che esulano dalle attività di consulenza, sorveglianza e, più in generale, consultazione, stabilite dall'art. 39 del GDPR – nonché, eventualmente, di tenuta del registro delle attività di trattamento (cfr. le Linee guida del WP29, par. 4.5, pp. 24-25).

12. Team del RPD | DPO

Come già richiamato nelle Linee guida del WP29 e nelle precedenti FAQ del Garante, in rapporto alle dimensioni e alla complessità dei trattamenti effettuati, occorre **valutare attentamente l'opportunità/necessità di istituire un apposito gruppo di persone (Team) a supporto del RPD | DPO**, al quale destinare le risorse necessarie allo svolgimento dei compiti stabiliti.

13. RPD | DPO interno e conflitti d'interesse

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

Associazione Data Protection Officer
Sede Legale: P.le Principessa Clotilde, 6 – 20121 Milano (MI)
Sede Operativa: Via Brianza, 65 – 22063 Cantù (CO)
info@assodpo.it - www.assodpo.it
C.F. 97656960156
P.IVA 08258580961 (solo per attività commerciale)

14. Incompatibilità del RPD | DPO – interno

Il tema dell'incompatibilità si presenta, quando il RPD|DPO:

- Rivesta incarichi quali quello di componente di un organismo collegiale (ad esempio, un comitato direttivo o un collegio disciplinare) o di titolare di un incarico monocratico dotato di poteri decisionali (es. vicepresidente, dirigente degli affari generali, direttore amministrativo)
- È figura già deputata ad assolvere altri specifici incarichi che comportano poteri decisionali in ordine a finalità e mezzi dei trattamenti posti in essere (es. in materia di trasparenza e/o di prevenzione della corruzione)
- È anche dirigente dell'unità organizzativa chiamata a curare la valutazione d'impatto sulla protezione dei dati relativa ad uno specifico trattamento (***direzione risorse umane, contabilità, il responsabile IT, o quella di dirigente dei dipartimenti che si occupano di conformità normativa, della gestione del rischio e di audit interni***)

15. Incompatibilità del DPO – esterno (es. società consulenza IT e legale).

Alla luce delle tante criticità insite nella scelta di affidare il compito di RPD | DPO ad un soggetto che già fornisce servizi al medesimo ente – con particolare riferimento a quelli del **settore IT** – **la principale soluzione consiste nel non designare**, quale RPD|DPO, soggetti a cui l'amministrazione affida un trattamento per suo conto, con conseguente necessità di definizione di un rapporto titolare-responsabile ex art. 28 GDPR; estendendo tale situazione anche a nomine a persone fisiche con ruolo e poteri nelle medesime società nominate responsabili del trattamento

Infatti questa sovrapposizione delle figure di RPD | DPO e di responsabile IT rende impossibile, di fatto, la sorveglianza e l'indipendenza che il cons. 97 del GDPR richiede in capo al RPD|DPO.

Medesima incompatibilità il GDPD rieleva nei confronti del legale che rappresenta in giudizio il Titolare del trattamento.

16. FAQ sul RPD | DPO in ambito privato

Il GDPD ha colto l'occasione anche per aggiornare le FAQ del settore privato, strumento molto più snello rispetto a quello pubblicato per il settore pubblico.

L'RPD | DPO è infatti di una figura chiamata ad assolvere funzioni di supporto, di controllo, consultive e formative, che deve essere adeguatamente coinvolta in tutte le attività che riguardano la protezione dei dati in azienda.

All'RPD | DPO non sono richieste specifiche attestazioni formali o l'iscrizione in appositi albi, deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di protezione dei dati personali, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento.

Maggiori approfondimenti al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793.

Milano | 31 maggio 2021

Approfondimento a cura di **Matteo Colombo**
Presidente ASSO DPO.