Mario Colantoni

IL DPO NELLE PUBBLICHE AMMINISTRAZIONI: CHI È E COSA FA?

www.sigiservizi.it

IL DPO NELLE PUBBLICHE AMMINISTRAZIONI: CHI È E COSA FA?

SOMMARIO

- ☑ Chi è il DPO?
- ☑ Requisiti del Data Protection Officer
- ☑ Funzioni e compiti del DPO nella Pubblica Amministrazione

CHI È IL DPO?

www.sigiservizi.it

IL DATA PROTECTION OFFICER

Il DPO o responsabile per la protezione dei dati personali (RPD) è una figura introdotta dal Regolamento GDPR (Reg. UE 679/2016). Si tratta di un soggetto designato dal titolare o dal responsabile del trattamento, al fine di coadiuvarli nella gestione dei trattamenti di dati personali da una posizione di autonomia e imparzialità.

La sua funzione è centrale nel garantire piena efficacia al principio di "*accountability*".

QUANDO È OBBLIGATORIO IL DPO

La **designazione** del DPO è **obbligatoria** (da parte del Titolare o del Responsabile del trattamento) solo se:

1.il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali;

2.le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;

3.le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'art. 9 o 10 GDPR.

LA NOMINA DEL DPO NELLE PUBBLICHE AMMINISTRAZIONI

- GESTIONE IN FORMA ASSOCIATA
- DPO INTERNO
- DPO ESTERNO

DPO INTERNO

- Nel caso in cui si opti per un RPD interno, sarebbe quindi in linea di massima preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, la designazione sia conferita a un dirigente ovvero a un funzionario di alta professionalità, che possa svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione.

- Necessario apposito atto di designazione

DPO ESTERNO

- Nel caso dei DPO esterno, le funzioni saranno esercitate sulla base di un contratto di servizi stipulato con una persona fisica o giuridica. Se la funzione di DPO è svolta da un fornitore esterno di servizi, i compiti stabiliti per il DPO potranno essere assolti efficacemente da un team operante sotto l'autorità di un contatto principale designato e "responsabile" per il singolo cliente. In tal caso, è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale DPO soddisfi tutti i requisiti applicabili come fissati nel GDPR.

- Necessario fare attenzione alla procedura di evidenza per la scelta del DPO (valore affidamento, requisiti partecipanti, SLA contratto)

DPO PERSONA GIURIDICA

Nel caso in cui una pubblica amministrazione affidi l'incarico di DPO ad una persona giuridica, il soggetto che viene designato quale DPO deve appartenere all'organico della persona giuridica, non essendo sufficiente una mera proposta d'incarico.

Tar Puglia - Lecce, sent. n. 1468/2019

GESTIONE IN FORMA ASSOCIATA

Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

(Art. 37, par. 3, GDPR)

I REQUISITI DEL DPO

www.sigiservizi.it

LE COMPETENZE DEL DPO

La certificazione di Auditor/Lead Auditor ISO/IEC/27001 non costituisce un titolo abilitante ai fini dell'assunzione e dello svolgimento delle funzioni di responsabile della protezione dei dati, nell'alveo della disciplina introdotta dal GDPR.

TAR Friuli Venezia Giulia, sent. n. 287/2018

LE COMPETENZE DEL DPO

- Figura **eminentemente giuridica** con conoscenza specialistica della normativa in materia di privacy e Data Protection italiana ed europea;
- Conoscenza dell'ente in cui il DPO viene nominato e **competenza in materia di procedure e regole amministrative**;
- Conoscenza tecnica dei sistemi IT.

IL RUOLO DEL DPO

- Il DPO va designato in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i propri compiti.

- È figura apicale, assolutamente diversa quanto a ruolo e funzioni dal "semplice" responsabile del trattamento.

- Può essere un dipendente del Titolare o del Responsabile del trattamento oppure un consulente esterno che assolve i suoi compiti in base a un contratto di servizi.

- I dati di contatto del DPO vanno comunicati al Garante per la protezione dei dati personali e resi pubblici.

AUTONOMIA E INDIPENDENZA

Il DPO deve essere autonomo ed indipendente:

- non deve ricevere dal Titolare o dal Responsabile alcuna istruzione per quanto riguarda l'esecuzione dei compiti affidati né è soggetto a potere disciplinare o sanzionatorio per l'adempimento dei propri compiti.

- deve avere le risorse necessarie e il potere di spesa per assolvere ai compiti assegnati, accedere ai dati personali e ai trattamenti e per mantenere le proprie conoscenze specialistiche (es. aggiornamento professionale).

FUNZIONI E COMPITI DEL DPO NELLA PUBBLICA AMMINISTRAZIONE

www.sigiservizi.it

COMPITI DEL DPO

- Informare e fornire al Titolare, al Responsabile nonché ai dipendenti che eseguono il trattamento, consulenza in merito agli obblighi normativi in materia;

- Sorvegliare l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche in materia del Titolare o del Responsabile del trattamento, compresi l'attribuzione di responsabilità, la sensibilizzazione e formazione del personale che partecipa al trattamento e al controllo in merito;

- Fornire, se richiesto, pareri sulla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

- Cooperare con l'Autorità di controllo e fungere da punto di contatto con il Garante per la protezione dei dati di personali per questioni connesse al trattamento.

Manuale RPD

Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea

(Regolamento (UE) 2016/679)

Elaborato per il programma "T4DATA" finanziato dall'UE

(Accordo di sovvenzione n°: 769100 — T4DATA — REC-DATA-2016/REC-DATA-2016-01)

di

Douwe Korff

Professore Emerito di Diritto Internazionale, Professore associato alla London Metropolitan University, alla Oxford Martin School e all'Università di Oxford

&

Marie Georges

Esperto indipendente sulla protezione internazionale dei dati (Ex-CNIL, Ue, Consiglio d'Europa, ecc.)

Membri del Gruppo FREE - Fundamental Rights Experts Europe

Con il contributo del Garante italiano per la protezione dei dati personali & dei Partner del progetto

(versione approvata dalla Commissione, luglio 2019)

COMPITI DEL DPO

Compito preliminare:

- ☑ Delineare il contesto in cui opera il titolare

Funzioni organizzative:

- ☑ Creazione e controllo di conformità del registro delle attività di trattamento;
- ☑ Verifica delle attività di trattamento dei dati personali;
- ☑ Verifica dei rischi posti dalle attività di trattamento;
- ☑ Gestione dei trattamenti che possono comportare un rischio elevato.

Controllo della conformità:

- ☑ Gestione delle violazioni dei dati personali;
- ☑ Compiti di indagine (compresa la gestione dei reclami interni).

COMPITI DEL DPO

Funzioni consultive:

- ☑ Consulenza sugli aspetti generali attinenti al trattamento dei dati personali;
- ☑ Sostegno e promozione dei principi di *privacy by design e protection by default*;
- ☑ Monitoraggio della compliance nel trattamento dei dati personali con specifica attenzione ai rapporti con tutte le figure coinvolte (contitolari, responsabili, altri titolari)

Cooperazione con il Garante per la Protezione dei Dati Personali

Gestione delle richieste degli interessati

Informazione e sensibilizzazione interna ed esterna

IL DPO E GLI INTERESSATI

Il RPD, se necessario con il supporto di un team di collaboratori, deve essere in grado di comunicare con gli interessati in modo efficiente e di collaborare con le autorità di controllo interessate. Ciò significa, fra l'altro, che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa.
Il fatto che il RPD sia raggiungibile – vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione – è fondamentale al fine di garantire all'interessato la possibilità di contattare il RPD stesso.

(Linee Guida Gruppo Art. 29)

RESPONSABILITA' DEL DPO

I DPO non rispondono personalmente in caso di inosservanza del GDPR. Quest'ultimo chiarisce che spetta al titolare o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del regolamento stesso (articolo 24, primo paragrafo). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare o sul responsabile.

(Linee Guida Gruppo Art. 29)

GRAZIE PER L'ATTENZIONE

www.lapadigitale.it

info@sigiservizi.it

www.sigiservizi.it