ANCE | ASSOCIAZIONE NAZIONALE COSTRUTTORI EDILI

Direzione Relazioni Industriali

PRIVACY
(Regolamento Europeo 679/2016 - operativo dal 25 maggio

Nota sulle Linee-guida sui responsabili della protezione dei dati (RPD/DPO)

Commento alle Linee-guida sui RPD/DPO

Le Linee Guida redatte dal Gruppo di lavoro articolo 29 (o Working Party art. 29, di seguito **WP29**)[1] offrono degli interessanti spunti per l'applicazione del nuovo **Regolamento generale per la protezione dei dati personali** (General Data Protection Regulation o **GDPR)** e per garantire una corretta *compliance* al medesimo.

* * *

Il Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO)

Il DPO rappresenta una figura di fondamentale importanza ai fini della responsabilizzazione (*accountability*) dei titolari del trattamento dati e per garantire un corretto adempimento alla normativa, aumentando anche il margine competitivo tra le imprese.

Il DPO rappresenta, infatti, un'interfaccia fra tutti i soggetti coinvolti nella gestione della privacy: autorità di controllo, interessati, divisioni operative all'interno delle aziende e degli enti e il Regolamento riconosce nel DPO un ruolo chiave nel nuovo sistema di *governance* dei dati.

È fondamentale rammentare che il DPO non risponde in caso di inosservanza del Regolamento, di cui rimangono unici responsabili il titolare e il responsabile del trattamento.

[1] Il WorkingParty29_Gruppo di lavoro articolo 29 è un organo europeo, istituito dalla Direttiva 95/46, che sarà sostituito dal nuovo Regolamento dal Comitato europeo per la protezione dei dati

Nomina del DPO

Il *Responsabile della protezione dei dati (RPD)* o *Data Protection Officer (DPO)*, chiamato a facilitare l'osservanza delle disposizioni del Regolamento della protezione dei dati (RGPD), può essere nominato dai titolari e dai responsabili del trattamento ed ha una funzione di intermediazione fra i soggetti coinvolti (autorità di controllo, interessati, divisioni operative all'interno delle aziende, etc.).

La nomina del DPO, pur essendo comunque consigliata dal WP29[2], è **obbligatoria** solo nei seguenti 3 casi:

1. se il trattamento è svolto da un'autorità pubblica/organismo pubblico;
2. se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono un monitoraggio regolare e sistematico di interessati su larga scala;
3. se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o dati personali relativi a condanne penali e reati.

Come avviene la nomina del DPO

Qualora la nomina del DPO ricada su un soggetto interno all'azienda/ente, occorre formalizzare un apposito atto di designazione del "Responsabile per la protezione dei dati", fornito dal Garante in occasione della pubblicazione delle FAQ relative al DPO.

In caso, invece, di ricorso a soggetti esterni all'ente, la designazione costituirà parte integrante dell'apposito contratto di servizi redatto in base a quanto previsto dal regolamento (art. 37).

Indipendentemente dalla natura e dalla forma dell'atto utilizzato, è necessario che nello stesso sia individuato in maniera inequivocabile il soggetto che opererà come DPO, riportandone espressamente le generalità, i compiti e le funzioni che questi sarà chiamato a svolgere in ausilio al titolare/responsabile del trattamento, in conformità a quanto previsto dalla normativa vigente.

L'eventuale assegnazione di compiti aggiuntivi, rispetto a quelli originariamente previsti nell'atto di designazione, dovrà comportare la modifica e/o l'integrazione dello stesso o delle clausole contrattuali.

Una volta individuato, il titolare o il responsabile del trattamento è tenuto a indicare, nell'informativa fornita agli interessati, i dati di contatto del DPO, pubblicando gli stessi anche sui siti web e a comunicarli al Garante, con apposito modello di comunicazione, anch'esso riportato in allegato alle FAQ di cui sopra.

[2] Tranne quando sia evidente che un soggetto non è tenuto a nominare un RPD, il WP29 raccomanda a titolari e responsabili di documentare le valutazioni compiute all'interno dell'azienda per stabilire se si applichi o meno l'obbligo di nomina del RPD.

Le "attività principali"

Con riferimento all'obbligo di nominare il DPO, nell'ipotesi in cui "le attività principali" del titolare o del responsabile consistono in trattamenti che richiedono un ***monitoraggio regolare e sistematico*** di interessati su ***larga scala***, è stato chiarito, primariamente, che, per ***attività principali*** si intendono le *operazioni necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento*.

Andrebbero comunque considerati anche i casi in cui il trattamento dei dati costituisce una componente inscindibile delle attività svolte dal titolare o dal responsabile (es. ospedale-*attività principale*: assistenza sanitaria; *attività inscindibile*: trattamento dati contenuti nelle cartelle cliniche).

Diversamente, le Linee Guida considerano le attività di pagamento delle retribuzioni al personale o la predisposizione di strutture di supporto informatico quali attività, seppur necessarie, né principali né inscindibili da queste e, presumibilmente, non suscettibili all'obbligo del DPO.

"Larga scala"

Pur non esistendo una precisa definizione di ***trattamento su larga scala*** nell'ambito del Regolamento, il WP29 ha fornito alcune indicazioni utili al fine di stabilire se un trattamento è effettuato su larga scala.

In particolare, per esaminare se un trattamento è su larga scala o meno, deve tenersi conto dei seguenti fattori:

- numero di soggetti interessati dal trattamento;
- volume dei dati e/o diverse tipologie dei dati oggetto del trattamento;
- durata dell'attività del trattamento;
- portata geografica dell'attività di trattamento.

A mero titolo esemplificativo, sono state, inoltre, indicate alcune ipotesi di trattamento su larga scala:

- trattamento di dati relativi a pazienti svolto da un ospedale;
- trattamento di dati relativi alla clientela di una compagnia assicurativa;
- trattamento di dati da parte di fornitori di sevizi telefonici o telematici.

"Monitoraggio regolare e sistematico"

Anche il termine monitoraggio non trova una definizione specifica nell'ambito del regolamento, dovendosi tuttavia intendere tutte le attività di profilazione e tracciamento on line e non solo.

Sul concetto di ***monitoraggio regolare,*** il WP29 ha precisato che deve intendersi tale ogni qualvolta lo stesso sia alternativamente:

- continuo o a intervalli definiti per un periodo di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- costante o a intervalli periodici.

L'aggettivo ***sistematico***, a giudizio del WP29, ha almeno uno dei seguenti significati:

- avviene per sistema;
- predeterminato, organizzato o metodico;
- ha luogo nell'ambito di raccolta dei dati;
- è svolto nell'ambito di una strategia.

Tra gli esempi di attività che comportano un ***monitoraggio regolare e sistematico*** devono intendersi le seguenti attività:

- reindirizzo di messaggi di posta elettronica;
- tracciamento dell'ubicazione da parte, ad esempio, di app su dispositivi mobili;
- utilizzo di telecamere a circuito chiuso;
- dispositivi per la domotica.

DPO del responsabile del trattamento

Il DPO può essere nominato dal titolare, dal responsabile o da entrambi.

Qualora il titolare sia tenuto alla nomina del DPO, non è detto che il responsabile sia ugualmente tenuto, pur costituendo buona prassi.

Nei casi di esternalizzazione del trattamento dati, ove l'***outsourcer*** sia responsabile del trattamento dati, quest'ultimo sarà tenuto alla nomina del DPO a differenza del titolare.

Designazione di un unico DPO per più organismi

La designazione di più DPO da parte di un gruppo imprenditoriale o di più enti collegati tra loro (possibile il riferimento a più enti bilaterali sul territorio) dipende dalla possibilità dello stesso di ***raggiungere facilmente*** ciascun membro del gruppo.

Il concetto di facilità deve essere legato al sistema di comunicazione adottato dal DPO e alla possibilità per lo stesso di fornire informazioni e consulenza ai diversi enti.

Chi può essere nominato DPO?

Con riferimento alle conoscenze e competenze specifiche del DPO, in mancanza di indicazioni tassative, le Linee guida offrono alcuni spunti di riflessione ai quali si rimanda, legati soprattutto al tipo di dati che vengono trattati, alla loro complessità e alla loro sensibilità.

Dovrà, poi, essere presa in considerazione una idonea qualità professionale con riguardo anche alla conoscenza della normativa e delle prassi europee in materia di protezione dei dati e un'approfondita conoscenza del Regolamento.

Ovviamente è utile anche la conoscenza dello specifico settore di attività e della struttura organizzativa.

Pubblicazione dei dati del DPO

I dati concernenti il DPO devono essere prontamente comunicati dal titolare o dal responsabile del trattamento per fare in modo che gli interessati (sia interni che esterni all'ente/organismo), il titolare e le autorità di controllo, possano contattarlo in maniera facile e diretta.

Si consiglia, ad esempio, nell'ambito di un'azienda o di un ente, di pubblicare il nominativo e tutti i dati di contatto del DPO (numero telefonico, indirizzo di posta elettronica, etc.) attraverso intranet.

Posizione del DPO

E' opportuno che il DPO sia sempre coinvolto nelle riunioni di medio-alto livello e, ogniqualvolta si debbano prendere decisioni che impattano sulla protezione dei dati, riceva sempre la opportuna considerazione. Secondo le indicazioni del WP29, in caso di disaccordo, dovranno essere opportunamente motivate le considerazioni che hanno portato a prendere condotte difformi da quelle raccomandate dal DPO.

Al DPO dovranno, inoltre, essere garantite le risorse necessarie all'assolvimento dei propri compiti (risorse finanziarie, formazione permanente, autonomia e indipendenza etc.).

Con specifico riferimento al concetto di ***"autonomia e indipendenza"*** è stato precisato che ciò consiste nella possibilità, sempre nell'esecuzione dei compiti attribuitigli, di agire senza ricevere istruzioni e riferendo direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento, senza poter essere rimosso o penalizzato da questi ultimi.

Può, inoltre, svolgere altre funzioni, purchè non diano adito a conflitti di interessi (ad es. ad un DPO esterno non si può chiedere di rappresentare in giudizio il titolare del trattamento su questioni inerenti la protezione dei dati).

Compiti del DPO

Il DPO, quale "punto di contatto" con l'autorità di controllo, deve primariamente ***sorvegliare l'osservanza*** del Regolamento (RGPD), pur non essendo personalmente responsabile in caso di mancato rispetto dello stesso (è responsabilità del titolare del trattamento mettere in atto tutte le misure per garantire e dimostrare che il trattamento è stato effettuato in modo conforme).

Non spetta, inoltre, al DPO condurre una valutazione d'impatto del trattamento dati (DPIA).

Il WP29 raccomanda, però, che il titolare si consulti con il DPO nella conduzione della DPIA e inserisca nel contratto, dandone anche comunicazione ai dipendenti, amministratori, etc., gli specifici compiti assegnati al DPO, soprattutto con riferimento alla DPIA.

Il DPO dovrebbe ***dedicare un'attenzione prioritaria agli ambiti che presentano maggiori rischi***, consigliando il titolare, sulla base di tale valutazione, la metodologia da seguire per la conduzione della DPIA e a quali trattamenti dedicare maggior tempo e maggiori risorse.

Pur rientrando nei compiti del titolare o del responsabile del trattamento, il DPO ***può tenere un registro dei trattamenti*** (come avviene di prassi), in quanto l'elenco delle attività affidate al DPO (di cui all'art. 39) è indicativo e non esaustivo.