Digital & Law
Department
www.studiolegalelisi.it

Chi è il Digital Protection Officer? La nuova figura professionale secondo i Garanti europei

COMMENTO ALLE LINEE GUIDA

Aggiornato al 1 febbraio 2017

Sommario

Digital & Law Department S.r.l.- via Vito Mario Stampacchia, 21 - 73100 Lecce
Tel. e Fax 0832/25.60.65 - e-mail: info@digitalaw.it

INTRODUZIONE

Il 24 maggio 2016, vent'anni dopo l'introduzione in Italia della prima Legge organica sulla protezione dei dati personali (Legge n. 675/1996), sostituita dal Codice Privacy (D.Lgs. n. 196/2003), è entrato in vigore il Regolamento europeo n. 2016/679 (General Data Protection Regulation – GDPR).

Il Regolamento abroga la Direttiva 95/46/CE, innestandosi nel *corpus* normativo vigente **senza comprometterne la validità e l'efficacia**: i principi, gli obiettivi e gli istituti del Codice Privacy, dunque, conserveranno – salvo modifiche - validità ed efficacia anche quando, dal 25 maggio 2018, il GDPR diventerà direttamente applicabile in tutti i Paesi UE.

Nondimeno, **la complessità e la portata innovativa** del sistema regolamentare europeo impongono all'interprete **un'analisi dettagliata e al contempo coordinata con la disciplina nazionale** e ai Titolari del trattamento – in particolare **professionisti, imprese e pubbliche amministrazioni** – una **ristrutturazione sistematica e multisettoriale del proprio assetto organizzativo**, uniformata ai **principi portanti della privacy by design e della privacy by default**.

È precisamente questa la ragione del differimento applicativo previsto dal Legislatore europeo: i soggetti che svolgono attività di trattamento di dati personali hanno a disposizione **un "periodo di adattamento", fino al 25 maggio 2018**, data in cui le nuove regole avranno **applicazione diretta e cogente nel nostro ordinamento** (così come in tutti gli Stati membri).

Per quella data, **l'allineamento alle prescrizioni del GDPR dovrà essere completa**, senza sconti: per rendere effettiva la "*protezione delle persone fisiche con riguardo al trattamento dei dati personali*" e "*la libera circolazione dei dati personali medesimi*", sono previsti **più penetranti poteri di controllo** in capo alle Autorità Garanti **e un inasprimento delle sanzioni pecuniarie** per un'ampia platea di soggetti, destinatari degli obblighi e delle responsabilità stabilite dal Regolamento.

È il caso, allora, di attrezzarsi per tempo, step by step: dalla **trasparenza informativa** alle **misure di sicurezza** (tecniche e organizzative), dalla **valutazione di impatto** ("**Privacy Impact Assessment**") alla tenuta dei **registri delle attività di trattamento**.

Ai nuovi adempimenti, corrispondono **nuovi ruoli soggettivi e professionali**, che affiancheranno gli attori del trattamento – Titolare, Responsabile e Incaricato – nell'assolvimento alle **funzioni di *compliance* e nella *governance* dei dati personali.**

Particolarmente rilevante, **tra le nuove figure introdotte dal GDPR** è il **Responsabile della Protezione dei dati personali o DPO ("*Data Protection Officer*"), la cui designazione è obbligatoria per tutti i soggetti pubblici e per alcuni soggetti privati**.

In proposito, il **Gruppo dei Garanti UE (WP 29)** ha adottato lo scorso 13 dicembre 2016 le **Linee Guida** recanti alcune indicazioni e raccomandazioni sull'applicazione delle **novità introdotte del Regolamento**, in vista dell'imminente applicazione da parte degli Stati membri.

Le linee guida, alla cui elaborazione ha partecipato anche il Garante Nazionale, consistono di tre documenti che riguardano, rispettivamente:

1. il Responsabile per la Protezione dei Dati ("Data Protection Officer" o "DPO");
2. il Diritto alla portabilità dei dati;
3. l' "Autorità capofila", che fungerà da "sportello unico" per i trattamenti transnazionali.

Digital & Law Department S.r.l.- via Vito Mario Stampacchia, 21 - 73100 Lecce
Tel. e Fax 0832/25.60.65 - e-mail: info@digitalaw.it

In particolare, le Linee Guida sul DPO chiariscono quali dovranno essere i requisiti soggettivi e oggettivi richiesti per ricoprire tale ruolo. Su questa tematica il Gruppo ha fornito preziose indicazioni soprattutto sui criteri che dovranno guidare le aziende nella designazione del DPO.

Il ruolo e i compiti del DPO

Per definire il ruolo del Responsabile della protezione dei dati individuato dal nuovo Regolamento, appare utile richiamare quali siano nello specifico i compiti che è tenuto a svolgere:

a) informare e consigliare il Titolare o il Responsabile del trattamento, nonché i dipendenti dell'organizzazione di appartenenza, in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) verificare l'attuazione e l'applicazione del Regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare o del Responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e i relativi audit;

c) fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;

d) fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;

e) fungere da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa.

In sintesi, dunque, dalle disposizioni contenute nel Regolamento europeo (art. 39 e Considerando n. 97) e nelle Linee guida del WP 29 emerge che il DPO dovrebbe:

- raccogliere informazioni per identificare le attività di trattamento;

- analizzare e verificare la conformità delle attività di trattamento;

- informare, consigliare e fornire raccomandazioni al Titolare e al Responsabile del trattamento.

La designazione del DPO

Uno dei primissimi argomenti esaminati nel documento in commento riguarda la "**designazione del DPO**". Il DPO è definibile come un **"attore chiave" nel nuovo sistema di *governance* dei dati** all'interno di PA e imprese ed è importante analizzare i casi in cui sia obbligatoria la nomina e quali siano gli adempimenti, nonché le "attività principali"[1] che ne derivano.

Anzitutto occorre operare una distinzione tra i due contesti: mentre per le amministrazioni e gli enti pubblici è obbligatorio nominare il DPO[2], le organizzazioni private dovranno designarlo solo qualora la loro attività principale consista in trattamenti che richiedano il controllo regolare e sistematico degli interessati o interessino dati di tipo sensibile. Alla luce di tale considerazione,

[1] Specificando cosa si intende per "attività principali" del Titolare o del Responsabile del trattamento, il WP ex art. 29 descrive alcuni settori che sarebbero obbligati alla nomina di un DPO: si tratta, ad esempio, delle aziende sanitarie (es. ospedali) o le società che forniscono un servizio di videosorveglianza a diversi soggetti (l'attività di sorveglianza viene considerata quale attività principale di queste società e questa viene indissolubilmente legata al trattamento dei dati personali). Alcune funzioni di supporto necessarie all'attività principale, poiché considerate accessorie, saranno escluse dall'obbligo di nomina di un DPO.

[2] Ad eccezione delle Autorità giudiziarie.

Digital & Law Department S.r.l.- via Vito Mario Stampacchia, 21 - 73100 Lecce
Tel. e Fax 0832/25.60.65 - e-mail: info@digitalaw.it

anche qualora le organizzazioni private non rientrino nell'obbligo, è necessario rimarcare come lo stesso Gruppo dei Garanti europei (WP 29) esorti ad avvalersi di un DPO.

La motivazione è semplice: da una parte il DPO può favorire all'interno del contesto organizzativo in cui opera il rispetto del Regolamento e, dall'altra, la sua presenza può generare un vantaggio competitivo per le imprese (in quanto soggetto posto a garanzia dei diritti e della tutela dei dati degli interessati, anche in virtù del suo ruolo di intermediario tra l'Autorità di controllo/interessati e l'organizzazione presso la quale svolge la propria attività professionale).

La sua designazione del DPO deve essere comunicata ufficialmente a tutto il personale dipendente, in modo che tutti sappiano dell'esistenza di questa nuova funzione all'interno dell'organizzazione e possano ricevere il supporto necessario in materia di *data protection*, consentendo, attraverso l'accesso alle informazioni, di facilitarne lo svolgimento dei compiti.

I Garanti europei hanno ulteriormente chiarito che, in base alla valutazione di alcune circostanze, il Titolare o il Responsabile del trattamento potranno essere obbligati, singolarmente o congiuntamente, alla nomina del DPO (in tal caso, i rispettivi DPO avranno l'obbligo di cooperare tra loro). Tuttavia, qualora l'obbligo ricada sul solo Titolare, non è detto che anche il Responsabile del trattamento sia, a sua volta, obbligato automaticamente alla nomina (sebbene ciò potrebbe costituire una buona prassi).

Il profilo del DPO

Il ruolo di DPO, può essere rivestito da una persona fisica, da un'organizzazione o da un team, in possesso di idonee competenze professionali.

Ai sensi dell'art. 37, par. 6, del Regolamento "il Responsabile della Protezione dei dati può essere un dipendente del Titolare del trattamento o del Responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi". Nelle menzionate Linee guida, sul punto si specifica che, considerato le dimensioni e la struttura dell'organizzazione, può essere necessario predisporre un team per il DPO. Allo stesso modo, in caso di esternalizzazione del servizio, il fornitore potrà ugualmente avvalersi di un team in grado di assolvere efficacemente i compiti di DPO, coordinato da figura responsabile di interfacciarsi nei rapporti con il cliente.

L'importante tema delle competenze e della formazione del DPO è oggetto delle menzionate Linee guida, in quanto il Titolare o del Responsabile del trattamento devono garantire un'adeguata e continua formazione in materia di protezione dei dati (mediante corsi di formazione, forum, workshop, etc.), affinché possa incrementare le sue competenze e mantenere adeguati livelli di aggiornamento.

La "raggiungibilità"

Qualora sia nominato da un gruppo di imprese o di enti pubblici, il DPO dovrà essere raggiungibile da ogni loro sede. In argomento, le Linee guida chiariscono che tale concetto di "raggiungibilità" è strettamente legato all'assolvimento dei compiti previsti dall'art. 39 del Regolamento: il DPO, oltre che al fungere da punto di contatto per i Titolari e i Responsabili del trattamento, dovrà essere in grado di comunicare in modo efficiente sia con tali soggetti che con le Autorità di controllo e le persone interessate al trattamento, oltretutto nella lingua o nelle lingue dalle stesse utilizzate nel luogo di stabilimento.

Digital & Law Department S.r.l.- via Vito Mario Stampacchia, 21 - 73100 Lecce
Tel. e Fax 0832/25.60.65 - e-mail: info@digitalaw.it

Le Responsabilità in ambito privacy

Dal punto di vista delle responsabilità, un DPO non può personalmente rispondere del mancato rispetto degli adempimenti previsti dal Regolamento per conto dell'organizzazione: sono il Titolare o il Responsabile del trattamento tenuti a garantire – e a dimostrare - che il trattamento avvenga in conformità alle disposizioni della normativa europea (art. 24 del Regolamento) e dunque a rimanere giuridicamente imputabili per eventuali responsabilità amministrative, penali e civili (nei confronti degli interessati).

Quello che resta in ogni caso imprescindibile è il coinvolgimento del DPO in tutte le questioni che potrebbero incidere sul corretto trattamento dei dati e, di conseguenza, il Titolare o il Responsabile devono garantire che:
• il DPO sia invitato a partecipare regolarmente alle riunioni tenute dal vertice gerarchico della struttura (es. dirigenti, quadri, etc.).
• il DPO sia presente nel momento in cui vengono prese determinate decisioni che hanno implicazioni sul trattamento e sulla protezione dei dati (in questo caso al DPO devono essere trasmesse tempestivamente tutte le informazioni necessarie affinché gli sia consentito di fornire una consulenza adeguata);
• siano tenuti nella debita considerazione tutti i pareri e le indicazioni forniti dal DPO (in caso di disaccordo (il WP29 raccomanda inoltre di documentare le ragioni che hanno portato i vertici dell'organizzazione a non seguire il consiglio del DPO);
• il DPO venga tempestivamente consultato qualora si verifichi una violazione dei dati personali o qualsiasi altro incidente che possa incidere sugli stessi (*data breaches*).

Titolari e Responsabili del trattamento, poi, al fine di rispettare i consigli dei Garanti europei, dovrebbero provvedere ad elaborare linee guida *ad hoc* o procedure aziendali interne in materia di protezione dei dati (es. Regolamenti interni), che stabiliscano i casi in cui un DPO deve essere obbligatoriamente consultato.

Cosa deve assicurare l'organizzazione al suo DPO?

Sia che si tratti di un contesto pubblico o di un contesto privato, il DPO deve godere delle dovute garanzie di indipendenza e inamovibilità nello svolgimento delle attività di indirizzo e controllo e, al contempo, gli devono essere fornite utili indicazioni per il corretto espletamento del suo ruolo. Come già sottolineato all'interno del Regolamento, inoltre, al DPO deve essere assicurato un sostegno adeguato in termini di risorse finanziarie, infrastrutturali (locali, strutture, attrezzature) e, se occorre, di coordinamento, a livello di risorse aziendali (personale).

Indipendenza e assenza di conflitti di interesse

Come stabilito dal Regolamento, inoltre, il DPO non deve ricevere alcuna istruzione e deve poter agire in maniera del tutto indipendente: questa enunciazione di principio, secondo i Garanti europei, si estrinseca nella libertà di consultare l'Autorità di controllo, fornire pareri e avere un'autonomia di visione riguardo ad un problema o all'interpretazione della legge; esiste però un limite: i suoi poteri decisionali non possono andare oltre quelli imposti dal Regolamento europeo (art. 39).

Strettamente legata alla necessità di agire in modo indipendente è il tema dell'assenza di conflitti di interesse all'interno dell'organizzazione, tematica che va a coprire una zona d'ombra relativa alla scelta del DPO. A tal proposito - a seconda delle attività, delle dimensioni e della struttura dell'organizzazione - i Garanti europei raccomandano di:

Digital & Law Department S.r.l.- via Vito Mario Stampacchia, 21 - 73100 Lecce
Tel. e Fax 0832/25.60.65 - e-mail: info@digitalaw.it

- individuare le posizioni interne che sarebbero incompatibili con la funzione di DPO[3];
- elaborare un apposito regolamento interno al fine di evitare eventuali conflitti di interesse;
- stabilire, in generale, le possibili attività che possono causare conflitti di interesse;
- dichiarare che il DPO da loro designato non ha alcun conflitto di interessi (per quanto riguarda lo svolgimento della sua funzione);
- introdurre specifiche garanzie attraverso regole interne all'organizzazione e predisporre contratti o accordi scritti (nei riguardi di chi andrà a ricoprire l'incarico di DPO) sufficientemente precisi e dettagliati, in modo da essere in grado di dimostrare, in caso di contestazioni (da parte di terzi), l'assenza di conflitto di interessi.

Il DPIA - Data Protection Impact Assessment

Infine, per precisare ulteriormente l'ambito di intervento del DPO nei vari e nuovi adempimenti imposti dal Regolamento europeo, viene definito il **ruolo che lo stesso deve avere nell'ambito della valutazione d'impatto sulla protezione dei dati (c.d. DPIA - *Data Protection Impact Assessment*)**.

I Garanti europei hanno specificato al DPO può essere richiesto un parere in merito a:

a) la necessità o meno di effettuare un DPIA;
b) la metodologia da seguire nello svolgimento di una DPIA;
c) l'esternalizzazione di questa attività;
d) le garanzie (comprese le misure tecniche e organizzative) da adottare per mitigare gli eventuali rischi per i diritti e gli interessi delle persone interessate al trattamento;
e) la correttezza di un DPIA e sulla conformità delle sue conclusioni al Regolamento.

Se il Titolare del trattamento non dovesse trovarsi in accordo con il parere fornito, occorrerà giustificare per iscritto la motivazione.
Ovviamente, i Garanti europei raccomandano altresì ai Titolari del trattamento di includere nel contratto stipulato con il DPO la descrizione dettagliata degli aspetti inerenti alla gestione dei compiti (compresa la loro portata) e alla realizzazione di un eventuale DPIA (fornendone anche notizia ai propri dipendenti).

Il registro delle attività di trattamento

Molto importante risulta essere anche l'ultima precisazione contenuta all'interno delle Linee guida in commento circa il **ruolo del DPO nella predisposizione, tenuta e aggiornamento del registro delle attività di trattamento** (obbligo imposto nei confronti di alcuni Titolari e/o Responsabili del trattamento ai sensi dell'art. 30 del Regolamento).

Si tratta, a ben vedere, di uno strumento che, raccogliendo una serie di informazioni fornite dai vari reparti di una determinata organizzazione, permette al DPO di svolgere i compiti di controllo della conformità e consulenza presso il Titolare o il Responsabile del trattamento.

Inoltre, sebbene la tenuta del registro non sia un compito specificatamente affidato al DPO ai sensi dell'articolo 39 del Regolamento, nulla vieta – secondo i Garanti europei – che gli possa essere ugualmente affidato. Occorre considerare che tale strumento consente il pieno controllo dei trattamenti, sia da parte del Titolare stesso sia da parte dell'Autorità Garante (in caso ne faccia richiesta), ed è in grado di fornire una panoramica delle attività di trattamento dei dati personali effettuate all'interno dell'organizzazione (pubblica o privata che sia). Il registro delle

[3] Si veda, da ultimo, l'Autorità Garante tedesca che ha dichiarato l'incompatibilità della funzione di DPO con chi già svolge il ruolo di IT Manager all'interno dell'organizzazione titolare del trattamento.

Digital & Law Department S.r.l.- via Vito Mario Stampacchia, 21 - 73100 Lecce
Tel. e Fax 0832/25.60.65 - e-mail: info@digitalaw.it

attività di trattamento, pertanto, viene considerato dal WP 29 un **prerequisito per la conformità al Regolamento** e, come tale, una **misura di "responsabilizzazione" efficace**.

Documento a cura del Team privacy – Digital & Law Department

Digital & Law Department S.r.l.- via Vito Mario Stampacchia, 21 - 73100 Lecce
Tel. e Fax 0832/25.60.65 - e-mail: info@digitalaw.it