Il ruolo del Data Protection Officer

Nomina, ruolo e compiti

Avvocato Luigi Guerra

Bari,17 novembre 2017 - Seminario Le novità del nuovo Regolamento Europeo sulla protezione dei dati

CSAD

CENTRO STUDI AMBIENTALI E DIREZIONALI

Dal **2002** ricerca e sviluppa **modelli formativi**

con la **finalità** di raccordarsi al sistema della Istruzione Pubblica e della Formazione Professionale pugliese,

integrando i percorsi di costruzione delle conoscenze e delle professionalità dei **professionisti**, del **personale** d'azienda, degli **imprenditori**, dei **giovani** laureati.

MISSION

Stimolare lo **sviluppo del tessuto imprenditoriale e dei professionisti** tramite **attività formative e informative** e **condividere iniziative di formazione** di eccellenza con **Università**, **Istituzioni** e **Organizzazioni** che si riconoscono in tale mission.

Data Protection Officer

Chi è il Data Protection Officer?

Siamo abituati alla scala gerarchica:

- Titolare;
- Responsabile;
- Incaricato;

Il DPO è un soggetto che facilita l'osservanza delle disposizione GDPR.

Il GDPR riconosce nel DPO uno degli elementi chiave all'interno del nuovo sistema di governance dei dati.

Riferimenti Normativi

- Articoli 37-38-39 GDPR;
- Linee-guida sui responsabili della protezione dei dati (DPO) adottate dal Gruppo di lavoro Art. 29, del 13 dicembre 2016;
- F.A.Q. allegate alle linee-guida;
- Scheda informativa Garante Privacy;

Obbligo designazione DPO

Art. 37 - LA DESIGNAZIONE DEL DPO È OBBLIGATORIA IN TRE CASI:

1. SE IL TRATTAMENTO È SVOLTO DA UN'AUTORITÀ PUBBLICA O DA UN ORGANISMO PUBBLICO (PROFILO SOGGETTIVO);

Esempio:

- Ente pubblico(le autorità statali, regionali o locali), P.A. e Ospedali;

Obbligo designazione DPO

2. SE LE ATTIVITÀ PRINCIPALI DEL TITOLARE O DEL RESPONSABILE CONSISTONO IN TRATTAMENTI CHE RICHIEDONO IL MONITORAGGIO REGOLARE E SISTEMATICO DI INTERESSATI SU LARGA SCALA (PROFILO OGGETTIVO);
3. SE LE ATTIVITÀ PRINCIPALI DEL TITOLARE O DEL RESPONSABILE CONSISTONO NEL TRATTAMENTO SU LARGA SCALA DI CATEGORIE PARTICOLARI DI DATI O DI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI.

Cosa significa "attività principali"? (art. 37, paragrafo 1, lettere b) e c)

Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento, comprese tutte quelle attività per le quali il trattamento dei dati è inscindibilmente connesso all'attività del titolare o del responsabile.

Esempio:

Il trattamento di dati relativi alla salute (come le cartelle sanitarie dei pazienti) è da ritenersi una delle attività principali di qualsiasi ospedale; ne deriva che tutti gli ospedali dovranno designare un DPO.

Obbligo designazione DPO

Cosa significa "su larga scala"? (art. 37, paragrafo 1, lettere b) e c)

Il regolamento non definisce cosa rappresenti un trattamento "su larga scala". Il WP29 raccomanda di tenere conto dei fattori qui elencati al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Alcuni esempi di trattamento su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;

Alcuni esempi di trattamento **non** su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Obbligo designazione DPO

Cosa significa "monitoraggio regolare e sistematico"? (art. 37, paragrafo 1, lettera b)

Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del GDPR; tuttavia, esso comprende senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale.

L'aggettivo **"regolare"** ha almeno uno dei seguenti significati a giudizio del WP29:

- che avviene in modo continuo ovvero ricorrente o ripetuto a intervalli costanti;

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

- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Qualche esempio:

- la prestazione di servizi di telecomunicazioni;
- profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi);
- tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili;
- programmi di fidelizzazione;
- monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili;
- dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

Nomina facoltativa DPO

Se si procede alla nomina di un DPO su base **volontaria**, troveranno applicazione tutti i requisiti di cui agli artt. 37-39 per quanto concerne la nomina stessa, lo status e i compiti del DPO esattamente come nel caso di una nomina obbligatoria.

CONSULENTE PRIVACY ESTERNO :

Nulla osta a che un'azienda o un ente, quando non sia soggetta all'obbligo di designare un DPO e non intenda procedere a tale designazione su base volontaria, ricorra comunque consulenti esterni privacy.

In tal caso è fondamentale garantire che non vi siano ambiguità in termini di denominazione, status e compiti di queste figure; è dunque essenziale che in tutte le comunicazioni interne all'azienda e anche in quelle esterne (con l'autorità di controllo, gli interessati, i soggetti esterni in genere), queste figure o consulenti non siano indicati con la denominazione di responsabile per la protezione dei dati (DPO).

Come faccio a sapere se sono obbligato o no a nominare un DPO?

Tranne quando sia evidente che un soggetto non è tenuto a nominare un DPO, il WP29 raccomanda a titolari e responsabili di documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se si applichi o meno l'obbligo di nomina di un DPO, così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti.

Tale analisi fa parte della documentazione da produrre in base al principio di responsabilizzazione (accountability).

Può essere richiesta dall'autorità di controllo e dovrebbe essere aggiornata ove necessario.

DPO esterno

Si può designare un DPO esterno? (art. 37, paragrafo 6)

Sì. In base all'art. 37, paragrafo 6, il DPO può far parte del personale del titolare o del responsabile del trattamento (DPO interno) ovvero "assolvere i suoi compiti in base a un contratto di servizi". In quest'ultimo caso il DPO sarà esterno e le sue funzioni saranno esercitate sulla base di un contratto di servizi stipulato con una persona fisica o giuridica.

Se il DPO è esterno, si applicano comunque tutti i requisiti fissati negli articoli da 37 a 39.

Per favorire efficienza e correttezza, le linee-guida raccomandano di procedere a una chiara ripartizione dei compiti nel team del DPO esterno, attraverso il contratto di servizi, e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente.

Designazione congiunta

E' ammessa la designazione congiunta di uno stesso DPO da parte di più soggetti? E a quali condizioni? (art. 37, paragrafi 2 e 3)

- E' consentito ad un gruppo imprenditoriale di nominare un unico DPO a condizione che quest'ultimo sia "facilmente raggiungibile da ciascuno stabilimento".

- Il concetto di raggiungibilità si riferisce ai compiti del DPO in quanto punto di contatto per gli interessati, l'autorità di controllo e i soggetti interni all'organismo o all'ente. Allo scopo di assicurare la raggiungibilità del DPO, interno o esterno, è importante garantire la disponibilità dei dati di contatto nei termini previsti dal GDPR.

- Il DPO deve essere in grado di comunicare con gli interessati in modo efficiente e di collaborare con le autorità di controllo interessate. Ciò significa 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 DPO 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 DPO stesso.

Quali sono le qualità professionali che un DPO deve possedere?

In base all'articolo 37, il DPO "è designato in funzione delle qualità professionali, in particolare della **conoscenza specialistica** della normativa in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39"

Fra le competenze e conoscenze specialistiche necessarie rientrano le seguenti:

- Conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, compresa un'approfondita conoscenza del GDPR;
- Familiarità con le operazioni di trattamento svolte;
- Familiarità con tecnologie informatiche e misure di sicurezza dei dati **(COMPETENZA INFORMATICA)**;
- Conoscenza dello specifico settore di attività e dell'organizzazione del titolare/del responsabile;
- Capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione del titolare/del responsabile.

NEWSLETTER DEL 15 SETTEMBRE 2017 GARANTE PRIVACY: gli attestati formali delle competenze professionali, non equivalgono a una "abilitazione" allo svolgimento del ruolo del DPO.

Posizione del DPO

COINVOLGIMENTO

Art. 38: titolare e responsabile assicurano che il DPO sia « **tempestivamente e adeguatamente coinvolto** in tutte le questioni riguardanti la protezione dei dati personali»

Ciò facilita l'osservanza del GDPR e il rispetto del principio di privacy fin dalla fase di progettazione (approccio standard)

E quindi:

- DPO sarà invitato a partecipare su base regolare alle riunioni manageriali di alto e medio livello;
- DPO sarà presente ogni volta che si assumono decisioni che impattano sulla protezione dei dati;
- Il parere del DPO deve ricevere sempre la dovuta considerazione. In caso di disaccordo , il WP raccomanda di documentare le motivazioni alla base di condotte difformi da quelle raccomandate dal DPO;
- DPO sarà consultato tempestivamente qualora si verifichi un data breach.

Posizione del DPO

RISORSE NECESSARIE

L'articolo 38 del GDPR obbliga il titolare o il responsabile a sostenere il DPO «**fornendogli le risorse necessarie** per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica».

Il DPO dovrebbe contare sulle seguenti risorse:

- Supporto attivo della funzione di DPO da parte del senior management;
- Tempo sufficiente per l'espletamento dei compiti affidati;
- Supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;
- Comunicazione ufficiale della designazione del DPO a tutto il personale;
- Accesso garantito ad altri servizi all'interno della struttura del titolare in modo tale da ricevere tutto il supporto, le informazioni o gli input necessari:
- Formazione permanente.

Posizione del DPO

LE GARANZIE DI INDIPENDENZA

Quali sono le garanzie che possono consentire al DPO di operare con indipendenza?

Vi sono numerose garanzie che possono consentire al DPO di operare in modo indipendente:

- Nessuna istruzione da parte del titolare o del responsabile per quanto riguarda lo svolgimento dei compiti affidati al DPO;
- Nessuna penalizzazione o rimozione dall'incarico in rapporto allo svolgimento dei compiti affidati al DPO;
- Nessun conflitto di interessi con eventuali ulteriori compiti o funzioni;

Il DPO non è rimosso o penalizzato dal titolare del trattamento od al responsabile per l'adempimento dei propri compiti.

Esempio: un DPO può ritenere che un determinato trattamento comporti un rischio elevato e quindi raccomandare al titolare o al responsabile di condurre una valutazione di impatto (DPIA), ma questi non concordano con il DPO. In casi del genere non è ammissibile che il DPO sia rimosso dall'incarico per aver formulato la raccomandazione in oggetto.

Posizione del DPO

LE INCOMPATIBILITÀ

Quali sono gli altri compiti e funzioni del DPO che possono comportare conflitti di interessi? (Art. 38, paragrafo 6)

Un DPO non può rivestire, all'interno dell'organizzazione del titolare un ruolo che comporti la definizioni delle finalità o modalità del trattamento dei dati personali.

Esempi di conflitto di interesse nei ruoli manageriali e di vertice:

- amministratore delegato;
- responsabile operativo;
- responsabile finanziario;
- direzione marketing;
- direzione risorse umane;
- responsabile IT.

Compiti del DPO

COMPITI DEL DPO:

- 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. (Informativa ex art. 13);
- Cooperare con l'Autorità di controllo, fungere da **punto di contatto per l'Autorità di controllo** oppure, eventualmente, consultarla di propria iniziativa;
- Considerare debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo;
- Fornire, se richiesto, **pareri in merito alla valutazione d'impatto sulla protezione dei dati** e sorvegliare i relativi adempimenti;
- Verificare che le policy interne del titolare siano correttamente applicate e attuate;
- Formazione costante del personale e audit interni.

Compiti del DPO

SORVEGLIARE

Che cosa rientra nel concetto di "sorvegliare l'osservanza" del regolamento? (art. 39, paragrafo 1, lettera b)

Fanno parte di questi compiti di controllo svolti dal DPO, in particolare:

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità al GDPR;
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

Compiti del DPO

VALUTAZIONE DI IMPATTO PRIVACY (DPIA)

In base all'art. 35, spetta al titolare del trattamento, e non al DPO, condurre, ove necessario, una valutazione di impatto sulla protezione dei dati (DPIA, nell'acronimo inglese).

Tuttavia, il DPO svolge un ruolo fondamentale e di grande utilità assistendo il titolare nello svolgimento di tale valutazione.

In ossequio al principio di "protezione dei dati fin dalla fase di progettazione" (o privacy *by design*), l'art. 35, prevede in modo specifico che il titolare "***si consulta***" con il DPO quando svolge una DPIA.

Il titolare o il responsabile dovrebbero consultarsi con il DPO, sulle seguenti tematiche:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento) siano conformi al GDPR.

Qualora il titolare non concordi con le indicazioni fornite dal DPO, è necessario che la documentazione relativa alla DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni.

Compiti del DPO

TENUTA DEL REGISTRO DEI TRATTAMENTI (Art. 30 GDPR)

In merito al registro dei trattamenti, la sua tenuta è un **obbligo** che ricade sul titolare o sul responsabile, **e non sul DPO (art. 30, primo e secondo paragrafo)**.

Niente vieta al titolare o al responsabile del trattamento di affidare al DPO il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare stesso. Tale registro va considerato uno degli strumenti che consentono al DPO di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare o del responsabile.

Avv. Luigi Guerra

Master Data Protection Officer Roma Tre
Consulente Privacy certificato TUV Italia cdp_149
Delegato Barletta-Andria-Trani Federprivacy

Contatti:

Studio: Via Canne n. 21 Barletta
Cellulare: 328/9699210
Email: guerra_luigi@yahoo.it

INFO, CONTATTI
E RICHIESTA ATTESTATI

CSAD Centro Studi Ambientali e Direzionali

Via delle Murge 65/A – 70124 BARI

Telefono: 080 5618455

Mobile: 348 7507598

Web: www.csad.it

Email: info@csad.it