La figura del Data Protection Officer nel nuovo Regolamento Europeo

Il Regolamento Europeo sulla protezione dei dati personali (General Data Protection Regulation, GDPR) prevede la figura del Data Protection Officer (DPO). La designazione di tale soggetto, oltre ad essere in alcuni casi obbligatoria, potrà portare benefici in termini focalizzazione sul rispetto della normativa e facilitazione delle iniziative ed attività necessarie per adempiere agli obblighi imposti dal Regolamento.

Questo documento affronta temi utili per operare le scelte necessarie per l'introduzione di questa figura, nuova per la normativa nazionale. In particolare i professionisti ed esperti, che hanno partecipato alla scrittura, hanno analizzato i requisiti normativi, la definizione del corretto posizionamento organizzativo e i rapporti con gli altri organismi di controllo (Collegio Sindacale, Organismo di Vigilanza, ecc.) e con l'autorità garante, presentando, in alcuni casi, le loro opinioni e interpretazioni in materia.

AIEA Associazione Italiana Information Systems Auditors
ISACA Capitolo di Milano

Introduzione al nuovo Regolamento Europeo 2016/679: figura del DPO e perimetro delle responsabilità

Il nuovo Regolamento Europeo sulla protezione dei dati personali 2016/679, “General Data Protection Regulation” (GDPR) pubblicato sulla Gazzetta ufficiale dell'Unione europea del 4 Maggio 2016 e che sarà applicabile dal 25 maggio 2018 dopo un periodo di transizione di due anni, intende rafforzare e unificare la protezione dei dati personali.

Gli obiettivi principali del GDPR sono di garantire ai cittadini il controllo dei propri dati personali e di armonizzare a livello europeo il contesto normativo attuale. A tal fine è stata adottata la forma del Regolamento e non della Direttiva, consentendo in tal modo l’applicazione di tutte le disposizioni normative nell'intera Unione Europea senza necessità del recepimento nelle legislazioni nazionali.

Fra le varie novità apportate, il GDPR ha previsto la figura del Data Protection Officer (DPO) o Responsabile della Protezione dei Dati, delineandone i compiti, le casistiche di designazione e i criteri di scelta per l’inserimento all’interno delle organizzazioni aziendali, fornendo così già a livello di disposizioni normative un set di indicazioni utili per individuare un professionista (o un team di esperti) che possa ricoprire adeguatamente tale ruolo.

La figura del DPO non è completamente nuova fra gli Stati Membri dell’Unione Europea, infatti alcuni di essi raccomandavano o in taluni casi imponevano (come la Germania ad esempio) già di procedere alla nomina di una figura simile al DPO. Ciò che mancava era un’armonizzazione a livello europeo che il nuovo Regolamento si propone di ottenere.

Attualmente la gestione della privacy in gran parte delle organizzazioni è demandata a figure non designate ad hoc, che provvedono a gestire gli adempimenti relativi al proprio ambito di competenza senza un coordinamento e una visione di insieme per quanto riguarda la protezione dei dati personali e il rispetto della normativa in ambito. Tipicamente le figure incaricate sono, ad esempio, l’IT manager o l’Head of Legal Department, a cui viene affidata anche questa responsabilità per le loro competenze professionali o la loro conoscenza dei flussi informativi aziendali.

Con la figura del DPO, formalmente designata ed identificata, si potrà avere:

- un unico soggetto avente la funzione controllo e monitoraggio per quanto riguarda l’adempimento dei requisiti dal nuovo Regolamento (ad esempio per l’esecuzione della valutazione d’impatto, la definizione del registro dei trattamenti, gestione delle terze parti ecc.);
- una figura in grado di agire da facilitatore tra le diverse funzioni aziendali che trattano dati personali e di gestire i rapporti con le parti interessate (interessati, autorità, ecc.);
- una maggiore attenzione alle iniziative necessarie per adempiere ai nuovi obblighi imposti dal Regolamento.

In ogni caso, tutte le principali funzioni aziendali (Information Security, Risk Management, IT, Legale, Compliance, HR, Internal Audit, ecc.) dovranno dare il loro contributo, relativamente all’area di propria pertinenza, al fine di implementare un modello di gestione della privacy operativo ed efficace nel tempo.

> L’introduzione della figura del DPO porta le organizzazioni in una delicata fase decisionale.

L’introduzione della figura del DPO porta quindi le organizzazioni in una delicata fase decisionale necessaria per determinarne il posizionamento all’interno dell’azienda e implementare le necessarie azioni organizzative e di processo finalizzate al rispetto dei requisiti indicati all’interno del GDPR.

La Designazione del Data Protection Officer

La designazione del Data Protection Officer è regolata dall’Articolo 37 del GDPR.

Il DPO deve essere designato sulla base delle qualità professionali, dell’approfondita conoscenza della normativa e delle prassi sulla protezione dei dati e della capacità di svolgere i compiti previsti all’Articolo 39, come indicato all’Articolo 37(5). Inoltre, il DPO deve possedere un background tecnico e organizzativo in merito al trattamento dei dati personali.

Il DPO dovrà rispondere al requisito di indipendenza e, nel caso gli siano affidati ulteriori compiti o funzioni rispetto a quelli specifici, non dovrà dare adito a conflitti di interessi (Articolo 38(6)).

WP29 - Guidelines on Data Protection Officers ('DPOs')

Si tratta di linee guida previste dal Regolamento stesso. Il documento prende in considerazione i casi in cui il DPO è obbligatorio, la posizione del DPO ed i suoi compiti.

E' inoltre disponibile un allegato con le risposte alle domande più frequenti (FAQ) e una traduzione in italiano di entrambi i documenti a cura del Garante per la protezione dei dati personali.

http://www.garanteprivacy.it/rpd

Il DPO è nominato dal Titolare del trattamento e dal Responsabile del trattamento; è prevista una designazione obbligatoria quando (Articolo 37(1)):

- il trattamento è effettuato da un'autorità pubblica o da enti pubblici, fatta eccezione per le autorità giudiziarie quando esercitano le loro funzioni giurisdizionali;
- le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, in virtù della loro natura, dell'ambito di applicazione e/o delle finalità, richiedono un monitoraggio regolare e sistematico delle persone interessate su larga scala;
- le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento su larga scala di categorie speciali di dati personali (*ex* articolo 9 del GDPR)[1] o di dati giudiziari relativi alle condanne penali e ai reati *ex* articolo 10.

Nella nomina del DPO è pertanto necessario distinguere i casi in cui il trattamento di dati personali è eseguito da una autorità pubblica o da enti pubblici dai casi in cui il trattamento è effettuato da operatori privati.

Nel primo caso il DPO viene obbligatoriamente designato dal Titolare e dal Responsabile del trattamento, ad eccezione delle autorità giudiziarie quando esercitano le loro funzioni giurisdizionali, indipendentemente dai dati personali trattati.

Per gli operatori privati, l'obbligo di nominare il DPO è previsto solamente nei casi in cui le attività principali del Titolare o del Responsabile del trattamento riguardino trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o quando le attività principali consistano in trattamenti, su larga scala, di categorie particolari di dati personali (origine razziale o etnica, opinione politica, convinzioni religiose o filosofiche, appartenenze sindacali, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o all'orientamento sessuale) o di dati relativi a condanne penali o reati.

L'Articolo 37(4) precisa che la nomina del DPO è obbligatoria anche in casi diversi da quelli sopra citati qualora prevista dalla legislazione dell'Unione e degli Stati Membri[2].

Qualora non si verifichino le condizioni sopra indicate, il DPO può essere nominato su base volontaria e si applicano i requisiti normativi specificati dagli Articoli 37, 38 e 39.

Il WP29[3] suggerisce che il Titolare e il Responsabile del trattamento documentino l'analisi svolta internamente per determinare la scelta di nominare o meno il DPO, dimostrando di aver opportunamente preso in considerazione i fattori rilevanti.

Il WP29 fornisce inoltre alcune indicazioni utili a interpretare nozioni citate ma non descritte dall'Articolo 37. Di seguito riportiamo in sintesi le principali:

- i concetti di "autorità pubblica" ed "ente pubblico" non sono precisati dal GDPR ma sono definiti dalla legislazione locale;
- secondo il WP29 le "attività principali" del Titolare e del Responsabile del trattamento sono le attività

[1] Dati sensibili, relativi alla salute o alla vita sessuale, genetici o biometrici, ecc..

[2] Il WP29, nel documento 16/EN WP 243 "Guidelines on Data Protection Officers ('DPOs')" del 13 dicembre 2016, evidenzia il fatto che la designazione di un DPO è normata anche dall'Art. 32 della Direttiva (UE) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, secondo cui "gli Stati membri dispongono che il titolare del trattamento designi un responsabile della protezione dei dati" e "possono esentare le autorità giurisdizionali e le altre autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali da tale obbligo."

[3] Il WP 29 o Art. 29 Working Party è un ente europeo di consultazione indipendente, istituito dall'art. 29 della Direttiva 95/46/CE, che raggruppa le autorità di protezione dei dati degli Stati membri. Si tratta di un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante Europeo della Protezione dei Dati), nonché da un rappresentante della Commissione.

primarie necessarie al raggiungimento degli obiettivi delle figure anzidette;
- anche la nozione di “regolare e sistematico” non è definita dalla norma. Il WP29 suggerisce di considerare il monitoraggio delle persone interessate “regolare” qualora avvenga con continuità o periodicamente, a specifici intervalli di tempo per uno specifico periodo, e “sistematico” se programmato, organizzato o metodico, oppure svolto come parte di una strategia o di un piano generale di raccolta dati. Rispondono a tali criteri, ad esempio, la fornitura di servizi di telecomunicazione, la profilazione e lo scoring svolti a fini di valutazione del rischio, la tracciatura della localizzazione, il monitoraggio dei dati di salute e benessere attraverso dispositivi indossabili.

Il DPO può essere un soggetto interno all’azienda oppure un soggetto esterno che assolve i propri compiti sulla base di un contratto di servizi.

Il DPO può essere un soggetto interno all’azienda, ossia un dipendente del Titolare o del Responsabile del trattamento, oppure un soggetto esterno che assolve i propri compiti sulla base di un contratto di servizi (Articolo 37(6)). Più in generale, la funzione di DPO può essere esercitata sulla base di un contratto di servizi stipulato con un professionista o con una organizzazione terza; all’organizzazione e a ciascuno dei suoi membri aventi ruolo di DPO si applicano le disposizioni di cui agli Articoli 37, 38 e 39, inclusi il requisito di assenza di conflitti di interessi e la garanzia che non siano attuate penalizzazioni (risoluzione del contratto di servizi o rimozione di un membro dell’organizzazione esterna) a causa dello svolgimento delle attività di DPO.

In caso di designazione di un team quale DPO, il WP29 raccomanda di definire una chiara allocazione dei compiti, individuando la persona con ruolo di contatto principale. In caso di organizzazione esterna, tali indicazioni potrebbero essere precisate nel contratto di servizio.

Un gruppo di imprese può designare un unico DPO, a condizione che sia facilmente raggiungibile da parte di ciascuno stabilimento (Articolo 37(2)). Più autorità pubbliche o organismi pubblici possono designare un unico DPO, tenendo conto della loro struttura e dimensione (Articolo 37(3)). D’altra parte, secondo il WP29, il Titolare o il Responsabile del trattamento devono assicurare che l’unico DPO possa svolgere i propri compiti in modo efficiente nonostante la sua responsabilità sia riferita a più entità, pubbliche o private.

Per assicurare che il DPO, interno o esterno, sia raggiungibile facilmente, in modo diretto e riservato dai soggetti interessati nonché dalle autorità di controllo, è necessario assicurare che i suoi dati di contatto siano resi disponibili dal Titolare o dal Responsabile del trattamento, in accordo all’Articolo 37(7).

La normativa, prevede che il Titolare e il Responsabile del trattamento designino un DPO ogniqualvolta vengano svolte attività o trattamenti di dati su “larga scala”. Non risulta tuttavia presente una definizione del concetto di “larga scala”, ad esempio in termini di numero minimo di trattamenti di dati personali.

A tale proposito, il “Considerando” 91 del GDPR indica come trattamenti su larga scala quelli che “mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala”; tuttavia “il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato”.

La nomina del DPO presuppone che allo stesso sia assicurata sufficiente autonomia e adeguate risorse, in termini di staff, budget e disponibilità di tempo, per svolgere i compiti assegnati dalla normativa (Articolo 38(2)).

Compiti e responsabilità del Data Protection Officer

L’Articolo 39 del GDPR affida al DPO, tra gli altri compiti ed implicitamente nel suo ambito di azione, quello di sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.

Nell’assolvere a tali funzioni il DPO può, in particolare:

- raccogliere informazioni per identificare le attività di trattamento,
- analizzare e verificare la conformità delle attività di trattamento, e
- informare, consigliare ed emettere raccomandazioni al Titolare del trattamento o al Responsabile del trattamento.

Controllo del rispetto della normativa non significa che il DPO sia personalmente responsabile in caso di non conformità. L'Articolo 38 del Regolamento richiede, tuttavia, che "il Titolare del trattamento e il Responsabile del trattamento si assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali".

Il GDPR esplicita che è il Titolare del trattamento e non il DPO, tenuto ad "attuare misure tecniche e organizzative per garantire e per essere in grado di dimostrare che il trattamento viene eseguito in conformità del Regolamento" e ne rappresenta il responsabile ultimo.

Di norma e in via generale, il DPO è incaricato di svolgere specifici compiti definiti dall'Articolo 39(1):

- informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, laddove richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento. Ai sensi dell'articolo 35, è compito del Titolare del trattamento, e non del DPO, l'effettuazione, quando necessario, di una valutazione dell'impatto sulla protezione dei dati. Tuttavia, il Titolare del trattamento deve richiedere il parere del DPO nello svolgimento dell'assessment;
- cooperare con l'autorità di controllo;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'Articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Il WP29 raccomanda che il Titolare del trattamento debba chiedere il parere del DPO, circa:

- la possibilità di effettuare o meno il Privacy Impact Assessment (PIA) e la metodologia da seguire nello svolgimento;
- la possibilità di effettuare il PIA in-house o se esternalizzare il servizio;
- i controlli da applicare per mitigare gli eventuali rischi per la salvaguardia dei diritti e degli interessi delle persone interessate, comprese le misure tecniche e organizzative;
- il parere circa il corretto svolgimento del PIA e se le sue conclusioni (di andare avanti o meno con le attività il trattamento, ad esempio) siano conformi al Regolamento.

Se il Titolare del trattamento non è d'accordo con le raccomandazioni suggerite dal DPO, dovrebbero essere specificamente giustificate per iscritto le motivazioni.

Qualità professionali del Data Protection Officer

Nell'eseguire i propri compiti il DPO considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo, come richiesto dall'Articolo 39(2).

La sua principale responsabilità è di verificare la gestione del trattamento di dati personali all'interno di un'organizzazione, affinché essa rispetti la nuova normativa UE, e deve fungere come punto di contatto per l'autorità di controllo per questioni connesse al trattamento e ad eventuali consultazioni. In definitiva, il DPO è un professionista con ruolo aziendale (sia esterno che interno) che deve possedere:

- adeguate competenze giuridiche;
- esperienza sulla legislazione relativa alla protezione dei dati personali sia nazionale che europea;
- conoscenza dei sistemi informativi e delle esigenze di sicurezza dei dati;
- comprensione dei processi di trattamento e delle tecniche di analisi dei rischi;
- conoscenza dei processi dell'organizzazione e del settore di business in cui questa opera.

Sebbene l'Articolo 37 del Regolamento non specifichi le qualità professionali che dovrebbero essere considerate al momento della designazione, emerge che il livello necessario di conoscenza specialistica del DPO dovrebbe essere determinato in particolare in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati (considerando 97 del GDPR). Il Titolare del trattamento o il Responsabile del trattamento dovrebbe essere assistito, dunque, da una persona che abbia una conoscenza specialistica della normativa e le competenze necessarie per vigilare che gli elementi essenziali del Regolamento siano implementati, quali:

- i principi del trattamento (Capo II);
- i diritti dell'interessato (Capo III);
- la protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (c.d. "data protection by design and by default") (Articolo 25);
- i registri delle attività di trattamento (Articolo 30);
- la sicurezza del trattamento (Articolo 32);
- la notifica e comunicazione di una violazione dei dati personali (Articoli 33, 34).

Quanto riportato per descrivere la figura del DPO apre nuovi scenari per la Pubblica Amministrazione e per i privati nell'individuare un professionista (o meglio, un team di esperti) che possa ricoprire adeguatamente un ruolo di fondamentale importanza nel garantire la protezione dei dati personali. E' del tutto evidente che tali figure dovrebbero avere pregressa e specifica esperienza nel settore della gestione dei dati ovvero in ambito legale in particolare nel settore della governance e compliance aziendali.

Il DPO in Germania e negli altri Stati Membri della UE

Nel seguito si riportano alcune indicazioni relativa alla normativa vigente in Germania perché in questo Stato la figura del DPO è già prevista come obbligatoria per legge con compiti e responsabilità definiti e circonstanziati.

A tal riguardo, la Germania prevede nella normativa attualmente vigente una distinzione fra elaborazione automatica e non-automatica di dati personali in modo da stabilire una designazione obbligatoria o meno del DPO. Nei casi in cui vi sia un'elaborazione automatica di dati vi è obbligo di designare il DPO, mentre nel caso di un'elaborazione non-automatica il DPO viene nominato solamente se vi sono almeno 20 impiegati aziendali.

In Germania la "Federal Data Protection Authority" ha come compito principale quello di verificare la compliance e sovrintendere il settore pubblico. Ogni Stato che appartiene alla Repubblica federale tedesca (16 Länder) ha un Data Protection Authority (DPA) il cui compito è verificare la compliance e sovrintendere il settore pubblico e privato. La Baviera è l'unico stato che ha istituito un DPA separato per il settore privato "Data Protection Authority of Bavaria for the Private Sector".

Per il settore privato il German Federal Data Protection Act, aggiornato nel 2009, costituisce la legislazione di riferimento, anche se esistono leggi di settore che contengono disposizioni relative alla protezione delle informazioni, ad esempio il Telecommunications Act. A causa dell'entrata in vigore del General Data Protection Regulation (GDPR) il Governo tedesco sta predisponendo un nuovo Federal Data Protection Act che recepisca le indicazionI del GDRP.

Il German Federal Data Protection Act stabilisce che un'azienda deve nominare un Data Protection Officer se al suo interno **almeno 10 dipendenti** sono coinvolti nel trattamento automatico di dati personali. La società può scegliere se nominare come DPO un dipendente o un consulente esterno, comunque il DPO deve possedere la conoscenza necessaria sulle leggi di data protection e deve essere affidabile e indipendente. La "Bavarian Data Protection Authority" ha recentemente ravvisato **un conflitto di interesse** nella nomina a DPO del **CIO di una società**[4]. Lo stesso conflitto di interesse è stato individuato nel caso in cui la nomina a DPO sia assegnata ad altri uffici pesantemente coinvolti nella gestione dei dati personali, come ad esempio **HR, Ufficio Marketing**.

Le attività della supervisory authority, così come sancite dall'articolo 38 del German Federal Data Protection Act prevedono:

- la verifica dell'applicazione della legge;
- la fornitura di consulenza e supporto ai DPO e ai controller (chiunque raccolga, processi o usi dati personali);
- l'esecuzione di ispezioni in loco;

[4] 20 ottobre 2016 https://globalcompliancenews.com/germany-data-protection-officer-conflict-of-interest-20161121)

- il monitoraggio dei data breach;
- il mantenimento di un registro;
- la delibera di misure per rimediare le violazioni individuate;
- il divieto di raccolta, trattamento o utilizzo dei dati personali in caso di serie violazioni o di ritardo nella realizzazione delle attività di correzione;
- la revoca del DPO se ritenuto non in possesso della necessaria conoscenza e affidabilità.

Il DPO (sezione 4g) deve assicurare la compliance al German Federal Data Protection Act e alle altre disposizioni in materia e deve, in particolare:

- controllare il corretto utilizzo dei programmi di elaborazione dati utilizzati per elaborare dati personali. A tal fine, il DPO deve essere informato in tempo utile dei progetti per il trattamento automatizzato dei dati personali;
- adottare misure appropriate per far conoscere alle persone impiegate nel trattamento di dati personali le disposizioni di legge e regolamentari.

Si riassume in tabella la regolamentazione della figura del DPO nei maggiori stati UE attualmente in vigore:

PAESE EU	DPO MANDATORY	DPO OPTIONAL
Austria		√
Belgio		√
Finlandia	all institutions giving healthcare and social welfare services must appoint a Data Protection Officer	√
Francia		√ Correspondant Informatique et Libertés or “CIL”
Germania	√	
Irlanda		√
Portogallo		√
Romania		√
Spagna		√
Svezia		√

Fonte: “International Comparative Legal Guide” (http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016)

La certificazione delle competenze del DPO

Il Regolamento UE incoraggia a più livelli l’adozione di codici di condotta e certificazioni come meccanismi ad esempio per dimostrare:

- il rispetto degli obblighi a carico del Titolare del trattamento;
- la conformità ai requisiti della Privacy by Design e by Default;
- la competenza sufficiente del Responsabile del trattamento nel mettere in atto misure tecniche e organizzative adeguate in modo tale che un trattamento soddisfi i requisiti del Regolamento medesimo;
- l’aver messo in atto da parte del titolare e del Responsabile del trattamento, misure tecniche e

organizzative adeguate per garantire un livello di sicurezza adeguato al rischio del singolo trattamento.

L'adozione di meccanismi di certificazione ha anche un impatto sulla determinazione dell'entità delle sanzioni per violazioni nel trattamento dei dati personali.

In questo scenario legislativo europeo di incentivazione alla diffusione ed adozione dei meccanismi di certificazione, anche la selezione e l'inserimento in azienda, di un DPO che possieda adeguati skill ed esperienze, valutati da una terza parte indipendente, può rappresentare un ulteriore elemento significativo a tutela del titolare del trattamento e del Responsabile del trattamento.

Tuttavia il DPO non è attualmente una figura professionale disciplinata dalla legge italiana.

Sul mercato sono disponibili degli schemi proprietari di riconoscimento delle competenze delle varie figure coinvolte nella gestione della privacy, solitamente gestiti da organismi di certificazione accreditati ma tali schemi non sono riconosciuti né a livello nazionale né a livello europeo e non hanno avuto finora una grande diffusione in Italia.

A livello nazionale, UNI - Ente Nazionale Italiano di Unificazione, organismo nazionale di normazione riconosciuto dall'Unione Europea ai sensi dell'articolo 27 del Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio sulla normazione europea, nell'ambito delle figure professionali non regolamentate (legge n.4 del 2013) in particolare per l'ICT ha predisposto un progetto di norma tecnica (E14D00036), attualmente in fase di inchiesta pubblica che individua e definisce i livelli di conoscenze, abilità e competenze di alcune delle figure potenzialmente coinvolte nella gestione e protezione dei dati personali.

Il progetto di norma titolato "Attività professionali non regolamentate – Profili professionali relativi al trattamento e alla protezione dei dati personali – Requisiti di conoscenza abilità e competenza" individua in particolare i seguenti profili nell'ambito del trattamento e della protezione dei dati personali. Il progetto di norma tecnica adotta il quadro europeo vigente di riferimento e di definizione delle competenze e delle relative abilità, in particolare la norma UNI EN 16234-1 e-Competence Framework (e-CF) oltre alla norma UNI 11506 (che definisce i requisiti relativi all'attività professionale delle figure che operano in ambito ICT) ed è stato pertanto elaborato in coerenza con il Quadro Europeo delle Qualifiche (European Qualification Framework – EQF, Raccomandazione 2008/C111/01).

Figure previste	**Descrizione:**
Responsabile della protezione dei dati personali	DPO come disciplinato in particolare dall'art. 39 del Regolamento Ue
Manager privacy	Soggetti con un elevatissimo livello di conoscenze abilità e competenze in uno specifico contesto organizzativo, che garantisce l'adozione di idonee misure organizzative nel trattamento dei dati personali
Specialista privacy	Figura a supporto del DPO e/o del Manager privacy
Valutatore privacy	Figura che svolge attività di audit con riferimento al trattamento e alla protezione dei dati personali

Modelli Organizzativi

Al fine dell'individuazione dei modelli organizzativi più idonei per il posizionamento del DPO si dovrebbero considerare:

- i requisiti del Data Protection Officer con impatti organizzativi;
- il conflitto di interesse nel ruolo del Data Protection Officer;
- il collocamento del Data Protection Officer.

I requisiti del Data Protection Officer con impatti organizzativi

Il GDPR, in particolare con l'art. 38: posizione del Data Protection Officer, e le linee guida del Working Party 29

(WP 29) relative alla figura del DPO ("*Guidelines on Data Protection Officers"*) definiscono specifici requisiti relativi al posizionamento del DPO all'interno delle organizzazioni.

Dalla lettura delle linee guida e dall'analisi dell'articolo 38 del GDPR emergono elementi utili ad individuare le responsabilità ed il ruolo del DPO e chiarire che la capacità di soddisfare i propri compiti deve essere interpretata non solo con riferimento alle qualità personali e di conoscenza del DPO, ma anche con riferimento alla sua posizione all'interno dell'organizzazione.

Tali elementi riguardano prevalentemente il suo coinvolgimento e interazione con le altre strutture interne all'organizzazione, le risorse necessarie per l'espletamento delle sue funzioni e la gestione dei conflitti di interesse. Al fine di identificare in modo corretto la posizione organizzativa del DPO in un contesto aziendale, è quindi fondamentale partire dall'analisi dei fattori che ne determinano il ruolo e le responsabilità all'interno dell'organizzazione.

Il DPO dovrà interagire con le altre funzioni organizzative, anche supervisionandone l'operato, in virtù della conoscenza specialistica della normativa, della protezione dei dati e della conformità al Regolamento.

L'art. 38 (1) del GDPR stabilisce che il DPO dovrà supportare il Titolare del Trattamento o il Responsabile del Trattamento anche nelle attività di cui non è diretto responsabile, supervisionandone l'operato, in virtù della sua conoscenza specialistica della normativa, della protezione dei dati e della conformità al Regolamento.

Inoltre, il suo parere dovrebbe sempre essere tenuto in considerazione e, in caso di disaccordo, sarebbe buona pratica istituire un processo di gestione del conflitto e documentare le ragioni per cui non sono state tenute in conto le sue raccomandazioni.

Per svolgere al meglio tale funzione, secondo l'art. 38 (3), il DPO deve riferire direttamente al vertice gerarchico del Titolare o del Responsabile dei trattamenti (solitamente Consiglio di Amministrazione o CEO).

Il DPO, in alcuni casi, è quindi il soggetto legittimato a interloquire ufficialmente con un soggetto esterno per conto del Titolare del trattamento, secondo l'art. 39 (1).

Inoltre, internamente all'organizzazione, il DPO deve essere coinvolto nell'ambito della governance aziendale al fine di essere visto come un partner di discussione all'interno dell'organizzazione e parte attiva all'interno dei gruppi di lavoro o attività progettuali inerenti l'elaborazione dei dati personali.

Tutte le informazioni devono, dunque, essere condivise con il DPO in modo tempestivo al fine di consentirgli di fornire un'adeguata consulenza, ad esempio con riferimento all'esecuzione della valutazione d'impatto sulla protezione dei dati o alla definizione del registro dei trattamenti. Il GDPR inoltre prevede esplicitamente il coinvolgimento del DPO sin dalle fasi iniziali (Privacy by Design) e specifica che debba essere chiesto il suo parere nello svolgimento di tale assessment.

Di conseguenza, il posizionamento organizzativo deve essere definito in maniera tale che il DPO:

- sia presente quando vengono prese decisioni con implicazioni sulle misure di protezione dei dati;
- sia invitato a partecipare regolarmente alle riunioni di senior e middle management (tavoli operativi riguardanti nuovi progetti di business e tavoli più formali dove potrebbe dar conto del suo operato) e a relazionare periodicamente in merito alla conformità dei trattamenti e all'andamento degli indicatori sulla protezione dei dati personali;
- sia facilmente raggiungibile tramite mezzi sicuri di comunicazione dagli interessati, ma anche all'interno dell'organizzazione, per tutte le questioni relative al trattamento dei loro dati personali e ai loro diritti presenti nel GDPR;
- funga da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva e consultazioni relative a qualunque altra questione.

L'art. 38 comma 2, del GDPR stabilisce che la società debba mettere il DPO nelle condizioni di operare fornendogli le risorse necessarie per assolvere ai suoi compiti, accedere ai dati personali, ai trattamenti e per mantenere la propria conoscenza specialistica.

A tal proposito l'organizzazione dovrà garantire al DPO:

- un supporto attivo e un adeguato impegno da parte del senior management (preferibilmente dal CdA);
- la garanzia che il ruolo e la funzione del DPO siano noti all'interno dell'organizzazione tramite comunicazione ufficiale a tutto il personale, ad esempio sulla intranet aziendale;

- il supporto in termini di risorse finanziarie e infrastrutture, in base alla grandezza e alla struttura dell'organizzazione, che gli consenta di valutare la necessità di risorse umane e strumenti adeguati per la protezione dei dati personali;
- l'adeguatezza del tempo a disposizione per l'adempimento dei propri compiti, calcolandolo sulla base delle responsabilità attribuitegli, in particolare nei casi in cui il DPO svolga anche altre funzioni;
- la possibilità di partecipare alla definizione di politiche e procedure per il trattamento e la protezione dei dati personali;
- la possibilità di definire un programma di verifica dei trattamenti;
- il supporto operativo delle altre funzioni aziendali, (Marketing, Risorse Umane, Legale, IT, Sicurezza, ecc.) per il raggiungimento degli obiettivi imposti dal Regolamento;
- la possibilità di formarsi e rimanere aggiornato per quanto riguarda gli sviluppi delle tematiche inerenti la protezione dei dati.

Il conflitto di interesse nel ruolo del Data Protection Officer

Come detto sopra il Titolare o il Responsabile, nel caso sia obbligato o decida autonomamente di nominare un DPO, dovrà assicurarsi che lo stesso adempia ai propri compiti in maniera **indipendente** *e* **riservata** interagendo, cooperando e fornendo la sua consulenza con integrità.

Affinché il DPO possa svolgere le proprie mansioni con un sufficiente grado di autonomia sia all'interno che all'esterno dell'organizzazione per cui opera, e nel caso il DPO svolga altri compiti e funzioni, è necessario che il Titolare o il Responsabile si assicurino che non vengano fornite a predetti individui indicazioni per l'esercizio della propria funzione, quali ad esempio:

- come affrontare questioni di interpretazione della normativa legislativa sulla protezione dei dati;
- quale sia il risultato da conseguire;
- quando consultare l'autorità di controllo.

E' necessario evitare situazioni di possibile conflitto derivanti da carichi di lavoro, posizione gerarchica o assunzione di altre responsabilità nella gestione dei dati personali.

È necessario che il Titolare o il Responsabile si assicurino che tali compiti e funzioni non determinino conflitti di interesse, quali ad esempio:

- conflitto di interesse correlato al tempo impiegato nell'adempimento alle mansioni di DPO e quello dedicato ad altri compiti e funzioni; tale tipologia di conflitto potrebbe essere accentuata nel caso in cui la valutazione del DPO tenga maggiormente conto delle mansioni e non del suo operato come tale nonché all'avvio di nuove attività cogenti richieste dal Regolamento stesso (es.: valutazione d'impatto sulla protezione dei dati, registro dei trattamenti, ecc.). Pertanto è opportuno che il DPO, per la stessa natura del ruolo e responsabilità che investe, non si trovi mai nella posizione di dover "sottrarre" tempo ai propri adempimenti a favore di altri compiti e funzioni;
- conflitto di interesse legato alla posizione gerarchica del personale impiegato nel supporto alle attività del DPO e nello svolgimento di altri compiti e funzioni; tale tipologia di conflitto potrebbe essere accentuato nel caso in cui, ad esempio, una risorsa della funzione IT, che collabora anche con il DPO, debba fornire raccomandazioni rispetto all'applicazione di una misura procedurale e/o tecnologica al responsabile della struttura organizzativa di appartenenza;
- conflitto di interesse correlato all'assunzione da parte del DPO di ruoli dirigenziali impattanti la gestione dei dati personali; tale tipologia di conflitto potrebbe essere accentuato nel caso in cui, nell'esercizio dei propri compiti e funzioni, il DPO debba indicare, suggerire o raccomandare, nell'ambito della Struttura Organizzativa di cui è responsabile, interventi specifici che impattano il trattamento dei dati personali, ad esempio, il responsabile della funzione IT, che riveste anche il ruolo di DPO potrebbe indicare, suggerire o raccomandare un'applicazione o una misura procedurale e/o tecnologica conveniente ai suoi scopi, ma meno conforme con la Normativa.

Collocamento del Data Protection Officer

Prima di identificare le aree dell'organizzazione più adatte al posizionamento del DPO, può essere utile identificare in quali aree non sia idoneo collocarlo, al fine di evitare conflitti di interesse come esplicitamente richiesto all'interno del nuovo Regolamento sulla

protezione dei dati personali, "*General Data Protection Regulation*" (GDPR) all'interno dell'art. 38, comma 6.

A seconda delle attività, delle dimensioni e della struttura dell'organizzazione, è buona prassi avere ben chiaro che il criterio principale per la valutazione del posizionamento del DPO all'interno dell'organizzazione è che tale ruolo non debba incorrere in nessun conflitto di interesse come nel caso dell'assegnazione di una posizione che abbia la facoltà di determinare le finalità e i mezzi del trattamento o una posizione che non garantisca un adeguato riporto gerarchico e la conseguente indipendenza e autonomia del DPO.

Il processo decisionale sul corretto posizionamento del DPO considera la possibilità di affidare tale ruolo ad un soggetto esterno o interno all'azienda. L'eventuale scelta di un posizionamento esterno del DPO potrebbe assicurare la riduzione di conflitti di interesse, potenzialmente dovuti ad una collocazione interna, tuttavia nella collocazione esterna è importante:

- definire puntualmente chi, all'interno dell'organizzazione, negozia e gestisce il contratto con la terza parte;
- verificare che la terza parte incaricata non abbia già altri contratti di consulenza attivi con l'organizzazione.

Come si evince dalle "*Guidelines on Data Protection Officers"* redatte dal WP 29, le posizioni interne all'organizzazione che potrebbero creare conflitti d'interesse per il posizionamento interno della figura del DPO includono ruoli di senior management quali ad esempio il Chief Executive Officer, Chief Operation Officer, Chief Financial Officer, il Chief Information Officer.

Queste figure sono sconsigliate in quanto, nell'ambito delle proprie attività ordinarie, potrebbero determinare le finalità e i mezzi del trattamento dei dati personali. L'elenco tuttavia non è esaustivo e, data la specificità di ogni organizzazione, è necessaria una valutazione caso per caso, identificando almeno:

- chi determina le finalità e i mezzi del trattamento dei dati personali;
- in quali aree vengono trattati i dati personali;
- quali tipologie di dati vengono trattati.

Successivamente per valutare correttamente il posizionamento del DPO è necessario:

- definire i criteri per il reclutamento del DPO;
- documentare l'analisi interna effettuata per identificare le posizioni che possono essere incompatibili con la funzione del DPO (ad esempio le posizioni o ruoli, all'interno dell'organizzazione, che concorrono alla determinazione delle finalità e modalità di trattamento dei dati);
- elaborare un Regolamento interno affinché il Titolare o il Responsabile siano in grado di dimostrare che i fattori rilevanti siano stati presi in considerazione correttamente.

Per minimizzare il rischio di conflitto d'interesse bisognerebbe collocare il DPO all'interno di un'apposita funzione creata ad hoc, prevedendo un riporto diretto ai massimi livelli gerarchici, come il CdA o il CEO. In linea con questa impostazione, già utilizzata in azienda per altri ambiti per cui è necessario garantire l'indipendenza e l'assenza di conflitti d'interesse, è la definizione degli Organismi di Vigilanza (OdV).

In alternativa, le funzioni all'interno di un'organizzazione più adatte a ricoprire tale ruolo, potrebbero essere quelle in cui non vengono determinate le finalità e i mezzi del trattamento dei dati personali, come ad esempio le aree di governance quali Compliance, Risk Management.

Nel caso in cui il Titolare del trattamento opti per un posizionamento interno, e nel caso in cui il DPO possa svolgere altri compiti e funzioni all'interno dell'organizzazione, sarà necessario inoltre valutare attentamente:

- il bilanciamento del tempo da dedicare alle diverse attività;
- il dimensionamento adeguato delle risorse a disposizione (staff, budget, ecc.) per l'esecuzione delle attività inerenti la protezione dei dati personali;
- il modello di reporting, quindi un flusso ordinario per le attività già in essere verso il diretto superiore e la definizione di nuovo flusso per la privacy verso i più alti livelli gerarchici (es. CdA e/o CEO).

Declinando operativamente quanto detto in precedenza sulla creazione di un'apposita funzione per il DPO o sul suo collocamento all'interno di una delle funzioni aziendali, un Titolare del trattamento che opera in un contesto multinazionale potrebbe, ad esempio, prevedere differenti ruoli:

- un Corporate DPO, che si occupi del controllo del modello privacy a livello di gruppo e coordini le relative attività operative necessarie. In caso di contesti caratterizzati da un'elevata complessità

organizzativa, trattamento di dati sensibili e da un'ampia estensione geografica dell'organizzazione potrebbe essere necessario affiancare al Corporate DPO diversi DPO regionali (ad esempio per ottemperare ai criteri di raggiungibilità del/dei DPO);
- referenti privacy per le diverse funzioni coinvolte nella gestione operativa del modello privacy definito (IT, Marketing, Legale, ecc.). Anche nell'ambito di tali ruoli potranno essere identificate figure locali sulla base dell'estensione geografica e della complessità dell'organizzazione.

La decisione in merito al modello organizzativo più adatto da adottare non risulta categorizzabile sulla base della industry di appartenenza del Titolare del trattamento, dal momento che i criteri di scelta identificati non evidenziano differenze sostanziali su aziende di diversi settori merceologici. Un diverso tipo di categorizzazione potrebbe riguardare invece la complessità dell'organizzazione, valutabile in termini di:

- tipologia di dati trattati (che potrebbero richiedere adempimenti più onerosi in termini di tempo e risorse, come ad esempio il trattamento di dati sensibili);
- dimensioni e complessità dell'organizzazione;
- distribuzione geografica dell'organizzazione.

Rapporti con altri organismi di controllo

Nei punti successivi si andranno a descrivere i possibili rapporti tra Il DPO e i principali Organi Societari, ovvero il Collegio Sindacale e l'Organismo di Vigilanza (…), e funzioni organizzative, tenuto conto che il DPO si delinea come una figura di controllo di secondo livello, volta a supervisionare e gestire le norme sulla protezione dei dati e le tecniche utilizzate per attuarla.

I possibili rapporti tra il DPO e i principali organi e funzioni devono tenere conto del fatto che il DPO si configura come una funzione di secondo livello.

Rapporti con Collegio Sindacale

Il Collegio Sindacale, è chiamato a vigilare (con atti di ispezione e controllo) sull'osservanza della Legge, dello Statuto e dei principi di corretta amministrazione, con particolare riguardo all'assetto organizzativo, amministrativo e contabile; vigila sul concreto funzionamento dell'organizzazione In alcune fattispecie (2409 bis 3°comma C.C.) esercita il controllo contabile.

Il DPO potrebbe, pertanto, riportare al Collegio Sindacale, periodicamente, un'informativa sul trattamento dei dati che abbia impatto sulla corretta amministrazione dell'organizzazione. Inoltre potrebbe informare il Collegio sull'aderenza delle politiche dell'organizzazione al Regolamento ed alle norme correlate al fine di scongiurare violazioni e, se pertinente, rendere noti i mezzi attraverso cui la protezione dei dati personali è svolta.

L'obiettivo del rapporto tra DPO e Collegio Sindacale è quello di contribuire a permettere a quest'ultimo una valutazione sull'amministrazione, sul rispetto dello statuto e sull'assetto organizzativo. A sua volta, il Collegio Sindacale potrà esprimere un parere sulla collocazione organizzativa del DPO al fine di valutarne l'indipendenza rispetto alle proprie funzioni, così come previsto dal GDPR.

Rapporti con Organismo di Vigilanza

L'organismo di Vigilanza, in conformità all'art. 6(1) del Decreto Legislativo 231/2001, ha il compito di vigilare sul funzionamento e l'osservanza del Modello di Organizzazione, Gestione e Controllo e di curare il suo aggiornamento.

L'introduzione della figura del DPO deve attivare l'Organismo di Vigilanza (ODV), il quale deve collaborare con esso al fine di aggiornare il Modello per le materie inerenti il trattamento e la protezione dei dati. In primis, è necessario valutare l'impatto che il nuovo Regolamento ha sul Modello adottato nell'organizzazione; quindi, calandosi nell'operatività dell'organizzazione, è necessario valutare i trattamenti adottati ad esempio alla luce dei reati informatici (Art 24 bis - Delitti informatici e trattamento illecito dei dati).

A regime, come nel rapporto con il Collegio Sindacale, il DPO informa periodicamente l'Organismo di vigilanza sui trattamenti in essere e sulla prevenzione di eventuali reati. Lo informa tempestivamente in caso di deviazioni dalla norma o di vere e proprie violazioni.

Da quanto sopra ipotizzato, il DPO si conferma essere, pertanto, una figura di controllo di secondo livello centrata sul monitoraggio del corretto trattamento dei dati all'interno della azienda, cui l'ODV deve rivolgersi per avere informazioni sul trattamento dei dati, sia a livello di adempimenti normativi, sia a livello, più

tecnico, di predisposizione delle sicurezze per il corretto trattamento.

Il DPO e la Funzione Compliance

Nelle disposizioni normative non vengono disciplinati i flussi informativi ed i rapporti tra il DPO e la Funzione Compliance, anche se l'interazione tra il DPO e la Funzione Compliance, il Risk Management e Internal audit è fondamentale per dare concretezza ad un sistema di controlli complessivamente idoneo ad assicurare la sana e prudente gestione dei rischi.

La Funzione di Compliance – che, come noto, è posizionata in maniera autonoma e indipendente rispetto alle altre funzioni – presidia il rischio di non conformità alle norme con riguardo a tutte le attività aziendali e assicura la verifica di secondo livello della corretta applicazione: i) delle regole interne alla società, ii) della corretta applicazione della normativa di riferimento emessa dalle Autorità di Vigilanza o obblighi di legge (ad esempio in ambito bancario la Funzione *compliance* assicura la corretta applicazione delle regole in materia bancaria in coerenza con il Regolamento Congiunto Banca d'Italia e Consob).

Nonostante, come detto, non vi siano indicazioni normative circa i rapporti e flussi informativi che possono strutturarsi tra la figura del DPO e la Funzione Compliance, per definire l'interazione fra la Funzione Compliance e il DPO è opportuno far riferimento *in primis* ai punti di contatto tra i soggetti quali:

- l'attività di informare il Titolare, il Responsabile del trattamento e i dipendenti che effettuano il trattamento;
- il presidio del rischio di non conformità al Regolamento UE, nonché ad altre normative nazionali;
- l'attività di fornire pareri.

Nell'ambito delle attività sopra esposte emergono ambiti di apparente sovrapposizione. Essa deriva dalle definizioni di Funzione di Compliance e DPO che presentano aspetti affini. Ciò nonostante, si ritiene che per tutte le attività in ambito privacy l'*owner* rimanga il DPO, ciò non toglie che – stante gli aspetti affini tra le attività – sarebbe auspicabile prevedere un flusso informativo strutturato tra i due soggetti e, in particolare, prevedere che la funzione *compliance* debba essere messa a conoscenza dell'attività svolta dal DPO.

Infatti il principale rischio in caso di sovrapposizioni o di attività affini è dato da una possibile contrapposizione all'interno delle funzioni di controllo che potrebbe – paradossalmente – esporre la società ad un rischio di non conformità. E' doveroso, pertanto, definire in modo chiaro che è il DPO l'*owner* del processo ma – al contempo – è doveroso sottolineare che spetta alla funzione *Compliance* un ruolo di primo piano come co-destinatario delle attività svolte dal DPO in particolare riguardo l'obbligo di informare il titolare, di presidiare il rischio e di fornire pareri.

> Il DPO e la Funzione di Compliance svolgono attività tra loro affini. E' opportuno, pertanto, stabilire l'*owner* delle diverse attività e determinare un flusso informativo chiaro tra le funzioni.

Non vi sono, invece, attinenze tra le due funzioni e il rapporto con il Garante. Tale flusso informativo verso il Garante spetta solo al DPO che – a seconda delle dimensioni aziendali – potrebbe stabilire di coordinarsi con la *business unit* (se presente) relazioni istituzionali.

I rapporti tra il DPO e la Funzione Internal Audit

La Funzione di Internal Audit effettua controlli di terzo livello ed esegue, fra l'altro, controlli *ex ante* ed *ex post* sull'adeguatezza e sull'efficacia della funzione di secondo livello tra cui la funzione *compliance* ed in particolare sul rispetto dei requisiti normativi di indipendenza e di autorevolezza.

La normativa non disciplina in alcun modo i rapporti tra il DPO e la funzione Internal Audit né specifica se la figura del DPO sia assimilabile ad un controllo di terzo livello o di secondo.

Ciò nonostante, a parere degli scriventi, tenuto conto dei compiti che vengono assegnati al DPO, questo potrebbe essere considerato più come una funzione di secondo livello che non una di terzo livello.

Pertanto i rapporti tra la funzione Internal Audit e il DPO possono essere paragonabili ai rapporti che sussistono tra la funzione di terzo livello e le funzioni di secondo livello.

Tutto ciò premesso pare ragionevole ritenere che la Funzione di Internal Audit – analogamente con l'attività svolta nei confronti della Funzione Compliance - ha il compito di verificare che il DPO svolga tutti i compiti a esso attribuiti e formalizzati nella policy e/o nel Regolamento, quali, a titolo esemplificativo e non

esaustivo rammentiamo i rapporti con il Garante, la gestione degli adempimenti normativi in materia di privacy, l'attività di informare il titolare e il responsabile. Tra le attività in capo alla Funzione Internal Audit rammentiamo anche quella di controllare il *reporting* della Funzione di secondo livello.

Verifica, infatti, la tempestività del *reporting,* la predisposizione dei flussi informativi previsti tra le Funzioni di secondo livello e le altre funzioni di controllo.

Infine pare, altresì, ragionevole ritenere che la funzione Internal Audit sia messa a conoscenza sugli esiti delle verifiche effettuate dal DPO.

I rapporti con la società di Revisione Contabile

La società di Revisione Contabile, così come previsto dalla normativa vigente, deve emettere un giudizio sul bilancio di esercizio della società attraverso controlli contabili.

Il DPO si prefigura come un interlocutore della Società di Revisione nella misura in cui il trattamento ha impatto sulle poste di bilancio: questi deve fornire chiarezza alla Società di Revisione sui trattamenti di dati personali svolti dall'azienda. Deve evidenziare in quali processi viene effettuato il trattamento e se possibili deviazioni da quanto previsto dal GDPR possono impattare sui dati di bilancio in termini di perdite o deterioramento delle poste.

Il DPO può essere la figura di riferimento per presentare il sistema di controllo per presidiare la compliance alla normativa privacy, come ad esempio le misure di sicurezza che l'azienda ha messo in atto al fine di prevenire un accesso a dati personali e un trattamento degli stessi non autorizzato (Accesso alle applicazioni, ai sistemi operativi ed ai database; protezioni dei dati, come cifratura di quelli sensibili, protezione delle reti perimetrali da attacchi esterni e interni). A tal fine deve collaborare con la società di revisione per garantire che questa abbia le informazioni necessarie per emettere un giudizio corretto sul bilancio.

Il DPO deve essere pertanto considerato tra le figure a disposizione della Società di Revisione per i controlli che questa deve svolgere al fine di assicurare un giudizio corretto sulla rappresentazione dei dati di bilancio. Il rapporto è quello di Controllo di terza parte-controllo di seconda parte. Si ritiene ci sia solo un flusso di informazioni dal DPO verso la società di Revisione Contabile.

Flussi informativi

Oltre al ruolo informativo e consultivo nonché al ruolo di *supervisor* dell'applicazione delle norme, interne ed esterne all'organizzazione, che regolano la protezione dei dati il DPO funge da:

- **centro di ricezione dei flussi informativi**, ovvero da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati personali o all'esercizio dei loro diritti [*rif. art. 38, punto 4*],
- **centro di trasmissione dei flussi informativi**, ovvero da punto di contatto per l'Autorità di Controllo per questioni inerenti il trattamento dei dati (ivi compresa la consultazione preventiva di cui all'art. 36 del Regolamento) o da richiedente consultazioni, inerenti qualunque altra questione riguardante la protezione dei dati personali, all'Autorità di Controllo;
- **centro di ricezione di richieste o comunicazioni da parte dell'Autorità.**

> I flussi informativi trasmessi dal DPO alle diverse entità sono strettamente correlati alla specifica *mission* che caratterizza tali interlocutori

In qualità di 'centro di trasmissione dei flussi informativi', il DPO annovera tra i suoi interlocutori entità di controllo societario quali il Collegio Sindacale, l'Organismo di Vigilanza, la Funzione *Compliance*, la Funzione *Internal Audit* e la Società di Revisione Contabile. In tale contesto di interrelazioni, i flussi informativi trasmessi dal DPO alle suddette diverse entità sono strettamente correlati alla specifica *mission* che caratterizza tali interlocutori e consentono di agevolare ed efficientare il loro processo di valutazione delle misure tecnico-organizzative adottate dalla Società per la protezione dei dati nei diversi ambiti di controllo:

- per quanto concerne i **rapporti con il Collegio Sindacale**, il DPO dovrebbe predisporre una informativa periodica atta ad aggiornare tale entità di controllo sul trattamento in essere dei dati che hanno impatto sulla corretta amministrazione della Società, con particolare riguardo all'assetto

organizzativo, amministrativo e contabile adottato e al suo concreto funzionamento. Inoltre, tale informativa dovrebbe informare il Collegio Sindacale sull'aderenza delle politiche societarie al Regolamento ed alle altre disposizioni, dell'Unione o degli Stati membri, relative alla protezione dei dati nonché, se pertinente, fornire una descrizione generale delle misure di sicurezza tecniche e organizzative implementate (art. 32, paragrafo 1 del Regolamento);

- relativamente ai rapporti con l'**Organismo di Vigilanza**, il DPO dovrebbe predisporre una informativa periodica atta ad aggiornare tale entità di controllo sul trattamento in essere dei dati che hanno impatto sul corretto funzionamento e sull'adeguata osservanza del 'Modello di Organizzazione, Gestione e Controllo' (in seguito "Modello") adottato dalla Società. Inoltre, tale informativa dovrebbe agevolare l'aggiornamento del Modello anche in relazione ai vigenti cambiamenti normativi in materia di protezione dei dati, fornire all'Organismo di Vigilanza una descrizione generale delle misure di sicurezza tecniche e organizzative implementate (art. 32, paragrafo 1 del Regolamento), anche in ottica di prevenzione di eventuali reati informatici, e informare tempestivamente l'entità di controllo su eventuali deviazioni dalla norma o di vere e proprie violazioni;
- per quanto concerne i rapporti con la **Funzione di Compliance**, il DPO dovrebbe predisporre una informativa periodica atta ad aggiornare tale entità di controllo sul trattamento in essere dei dati che hanno impatto sulla corretta gestione dei rischi *privacy*. Inoltre, tale informativa dovrebbe informare la Funzione di Compliance sull'aderenza delle politiche societarie al Regolamento ed alle altre disposizioni, dell'Unione o degli Stati membri, relative alla protezione dei dati nonché, se pertinente, fornire una descrizione generale delle misure di sicurezza tecniche e organizzative implementate di cui all'art. 32, paragrafo 1 del Regolamento;
- relativamente ai rapporti con la **Funzione Internal Audit**, il DPO dovrebbe predisporre una informativa periodica atta ad aggiornare tale entità di controllo rispetto i trattamenti dei dati coinvolti nelle attività dal medesimo svolte e previste dal Regolamento (ad esempio i rapporti con l'Autorità Garante della Privacy/ Autorità di Controllo, la gestione degli adempimenti normativi in materia di *privacy*, l'attività di informare e formare il Titolare del Trattamento e il Responsabile del Trattamento, ecc.);
- per quanto concerne i rapporti con la **Società di Revisione Contabile**, il DPO dovrebbe predisporre, ogni qualvolta le sia richiesto (ad esempio durante i controlli propedeutici alla emissione del giudizio sul Bilancio), una comunicazione atta ad aggiornare tale entità di controllo in merito alle misure di sicurezza che l'azienda ha messo in atto al fine di prevenire un accesso ai dati personali e sensibili e un trattamento degli stessi non autorizzato (art. 32, paragrafo 1 del Regolamento)

Rapporti con il Garante

L'art. 39 del GDPR attribuisce al DPO, tra l'altro, il compito di cooperare e di fungere da punto di contatto con l'autorità di controllo. Per inquadrare meglio tali compiti e per contestualizzarli nella realtà operativa delle imprese, si riportano di seguito le principali fattispecie di interazione tra titolare del trattamento e autorità così come previste dall'attuale normativa e dal GDPR.

Verifica preliminare

L'art. 17 del codice privacy prevede la possibilità, nel caso di trattamenti di dati che presentano rischi specifici, di richiedere una verifica preliminare del Garante.

In pratica, l'istanza va corredata con una relazione che riporti una descrizione generale del progetto, spieghi nel dettaglio i trattamenti di dati personali che si intendono effettuare (canali di acquisizione dei dati, finalità e modalità del trattamento, tempi di conservazione, ecc.) e indichi le misure previste in relazione ai rischi per la privacy degli interessati.

Il Regolamento del Garante prevede un tempo massimo di 180 giorni per l'istruttoria, al termine della quale l'autorità può, alternativamente, approvare il progetto, prescrivere misure aggiuntive, o indicare che il progetto non è sostenibile dal punto di vista privacy.

Analogamente, l'art. 36 del GDPR prevede la consultazione preventiva dell'autorità, qualora la valutazione d'impatto sulla protezione dei dati svolta dal titolare consultando il DPO ove designato, indichi che il

trattamento presenterebbe un rischio elevato, in assenza di misure adottate per attenuarlo.

Richieste di autorizzazioni

Il codice privacy prevede diversi casi in cui il titolare deve richiedere una autorizzazione specifica del Garante, prima di poter procedere con il trattamento dei dati. In particolare:

a) quando il trattamento è svolto per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti o un legittimo interesse dell'interessato (c.d. bilanciamento di interessi - art. 24 del codice privacy);
b) per il trattamento di dati sensibili, al di fuori dei casi già individuati nelle autorizzazioni generali pubblicate dal Garante (art. 26 del codice privacy);
c) per il trasferimento di dati personali verso Stati extra-UE, basato su clausole contrattuali definite autonomamente dal titolare o sulle c.d. “binding corporate rules” (art. 44 del codice privacy). Queste ultime fattispecie sono previste anche dal GDPR (artt. 46 e 47).

Notificazione dei trattamenti

Ai sensi dell’art. 37 del codice privacy, devono essere preventivamente notificate al Garante determinate tipologie di trattamenti di dati personali, ad esempio riguardanti dati genetici, biometrici, profilazione con strumenti automatizzati, ecc.

In pratica, la notificazione avviene tramite un form online, pubblicato nella specifica sezione del sito del Garante, che va compilato e sottoscritto con firma digitale.

Il GDPR non prevede più questo adempimento.

Adempimenti in caso di violazione della sicurezza dei dati personali (data breach)

Ad oggi, secondo l’art. 32-bis del codice privacy, solo i fornitori di servizi di comunicazione elettronica (telco e ISP) sono tenuti ai seguenti adempimenti, in caso di data breach:

- comunicazione al Garante entro 24 ore di ogni data breach occorso;
- comunicazione ai clienti, o altri soggetti coinvolti, entro 3 giorni, se la violazione può recare pregiudizio ai loro dati personali o alla loro riservatezza;
- tenuta di un registro dei data breach avvenuti.

L’art. 33 del GDPR prevede adempimenti simili per tutti i titolari del trattamento, indipendentemente dal settore di attività, seppur con termini meno stringenti (ad esempio, la comunicazione all’autorità è prevista entro 72 ore anziché 24, ecc.). La notifica all’Autorità contiene il nome ed i dati di contatto del DPO ove designato, che assume un ruolo fondamentale diventando il punto di contatto per ottenere maggiori informazioni.

Accertamenti e controlli del Garante

Per l'espletamento dei propri compiti, il Garante può richiedere, ai sensi dell’art. 157 del codice privacy, di fornire informazioni e di esibire documenti, per esempio a seguito di reclami o segnalazioni da parte dei cittadini, ecc.

Inoltre, l’art. 158 del codice privacy prevede che Il Garante può disporre accessi a banche di dati, archivi o altre ispezioni e verifiche. A tal fine, il Garante dispone di un proprio nucleo ispettivo e, inoltre, ha stipulato una convenzione con la Guardia di Finanza, che effettua a sua volta ispezioni in ambito privacy.

Conclusioni

Il Regolamento Europeo sulla protezione dei dati personali 2016/679, “General Data Protection Regulation” (GDPR), che sarà applicabile dal 25 maggio 2018, dopo un periodo di transizione di due anni, intende rafforzare e unificare la protezione dei dati personali a livello Europeo. Fra le varie novità apportate, il GDPR ha previsto la figura del Data Protection Officer (DPO), delineandone i compiti, le casistiche di designazione e i criteri di scelta per l’inserimento all’interno delle organizzazioni aziendali. Le questioni che la scelta di tale figura pone non sono poche né è sempre possibile individuare, anche in ragione della novità normativa, una chiara guida interpretativa. Di particolare rilevo appare la decisione di individuare il DPO internamente o esternamente (sottoscrivendo un contratto di servizi) all’organizzazione, come singolo o come team, e la collocazione organizzativa che ne consenta la piena operatività, evitando nel contempo possibili conflitti di interesse.

Se correttamente implementata la figura del DPO, formalmente designata ed identificata, porterà benefici sia a livello normativo sia nell’ambito delle organizzazioni in cui opererà. In particolare ad esso è assegnata una funzione di controllo e monitoraggio sull’adempimento dei requisiti del Regolamento, ma potrà anche rivestire il ruolo di facilitatore all’interno delle organizzazione delle iniziative e delle attività necessarie per adempiere, in modo sostenibile, agli obblighi imposti dal Regolamento.

.

Ringraziamenti

Un sincero ringraziamento per aver realizzato questo documento, mettendo a disposizione il proprio tempo e le proprie conoscenze a:

Giuseppe Blasi (Protiviti)

Silvia Bertini (Istituto Italiano di Tecnologia)

Elisa Faccioli (Unione Fiduciaria)

Giovanni Ferrandu (Unione Fiduciaria)

Marcello Fumagalli (Unione Fiduciaria)

Andrea Gaglietto (Protiviti)

Giovanni Giammanco (Eni)

Alessandro Gisolfi (KPMG)

Luca Lumini (DXC Technology)

Marco Mancini (Enel)

Giuseppe Mantese (Dottore Commercialista)

Andrea Mariotti (Ernst&Young)

Margherita Mezzacapo (Enel)

Leonardo Nobile (DXC Technology)

Pietro Nieddu (KPMG)

Nicola Paolino (KPMG)

Clarice Rosa (Intesa Sanpaolo)

Luca Savoia (Mazars)

Stefano Tagliabue (TelecomItalia)

Silvia Valenti (Allianz)

Un ulteriore ringraziamento particolare a Luca Savoia per aver promosso l'idea di questo lavoro nell'ambito dell'Associazione.

Simona Napoli

Vice presidente AIEA

Maggio 2017