XIV INCONTRO COMPLIANCE

"IL REGOLAMENTO EUROPEO UE 2016/679 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI: LE PRINCIPALI NOVITÀ PER IMPRESE E SOGGETTI PUBBLICI"

IL DATA PROTECTION OFFICER: ASPETTI ORGANIZZATIVI E FUNZIONALI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI

Claudio Coratella *Name Partner, Coratella - Studio Legale*

CHI E' IL DATA PROTECTION OFFICER?

- Il Data Protection Officer (di seguito "**DPO**"), già presente in alcune legislazioni europee, è una figura introdotta dal Regolamento generale sulla protezione dei dati 2016/679 | GDPR, pubblicato sulla Gazzetta Ufficiale europea L. 119 il 4 maggio '16.

- Il DPO, è un professionista che deve avere un ruolo aziendale (sia esso soggetto interno o esterno) con competenze giuridiche, informatiche, di risk management e di analisi dei processi.

CHI E' IL DATA PROTECTION OFFICER?

- Il suo compito principale è quello di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.
- Il DPO è l'evoluzione del "privacy officer", figura prevista dalla direttiva europea 95/46 laddove, all'art. 18, consentiva agli Stati dell'Unione di prevedere semplificazioni o esenzioni nei casi di designazione di un soggetto indipendente che garantisca l'applicazione della normativa.

CHI E' IL DATA PROTECTION OFFICER?

- Il DPO, quindi, è un consulente esperto che assiste il titolare nella gestione delle problematiche del trattamento dei dati personali.

- In tal modo si garantisce che un soggetto qualificato si occupi, in maniera esclusiva, della materia della protezione dei dati personali, aggiornandosi sui rischi e le misure di sicurezza, in considerazione della crescente importanza e complessità del settore.

Chi è tenuto a nominare il DPO?

- Il Regolamento sulla Data Protection, entrato in vigore il 25 maggio 2016, applicabile a tutti i 28 Stati membri UE a decorrere dal 25 maggio 2018, all'art. 37, disciplina l'istituzione della figura del Data Protection Officer (in italiano Responsabile della protezione dei dati) nei seguenti casi:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

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

Chi è tenuto a nominare il DPO?

c) le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 (dati particolari | sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10.

- L'articolo 9 del Regolamento al comma 1 definisce quelli che sono le categorie particolari di dati personali (ex dati sensibili) ed in particolare i dati personali che: "rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".

Chi è tenuto a nominare il DPO?

1. «Autorità pubblica o organismo pubblico»

In merito all'ipotesi sub a), nel regolamento non si rinviene alcuna definizione di "autorità pubblica" o "organismo pubblico".

Il Working Party ritiene che tale definizione debba essere interpretata conformemente a (ciascun) diritto nazionale.

Tuttavia, è bene evidenziare che nelle Linee guida del 13 dicembre 2016 viene "raccomandata" la nomina del DPO anche per quegli "organismi privati incaricati di funzioni pubbliche o che esercitano pubblici poteri“.

Chi è tenuto a nominare il DPO?

Il Working Party rammenta, inoltre, che, una volta nominato, il DPO dovrebbe svolgere la propria attività non solo con riguardo ai trattamenti strettamente connessi all'espletamento di funzioni pubbliche ma anche ad altre attività quali, per esempio, la gestione di un database del personale.

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata.

I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Chi è tenuto a nominare il DPO?

2. «Attività principali» o «core activities»

- Le «core activities» non vanno intese soltanto come le attività tipiche (o «primarie») del titolare o del responsabile.

- Esse includono, altresì, tutto ciò che, con le attività primarie, si trova «inestricabilmente connesso».

Chi è tenuto a nominare il DPO?

- Per chiarire meglio il punto: attività tipica o primaria di una struttura sanitaria privata non è quella di trattare i dati sensibili dei pazienti, ma di fornire prestazioni sanitarie. Tuttavia, è evidente che questa attività presuppone necessariamente il trattamento dei dati sanitari dei pazienti, diversamente non potrebbe essere svolta.

- Dunque, il trattamento dei dati sensibili costituisce qui *core activity* e concorre a determinare l'obbligo di designare il DPO.

Chi è tenuto a nominare il DPO?

- Altro esempio è quello della fornitura di servizi di videosorveglianza: senza trattamento dei dati personali (nella specie immagini ed eventualmente audio, trasmessi e/o registrati dalle videocamere), l'attività tipica non può essere prestata.

- Non sfugge all'interprete che l'espressione «inextricable part» scelta dal Gruppo di lavoro richiama immediatamente analoga terminologia utilizzata dalla Corte di Giustizia UE a proposito dell'applicazione territoriale della (tuttora vigente) direttiva 95/46/CE, cfr. CGUE, Google Spain, C-131/12, § 56 («inextricably linked»).

Chi è tenuto a nominare il DPO?

- Secondo l'impostazione dei Garanti, non è invece considerata *core activity* ma mera «attività ancillare» quella relativa al pagamento dei dipendenti o quella di gestione ordinaria delle risorse informatiche. Come tale, essa è irrilevante ai fini della designazione del DPO.

- L'esempio scelto non è dei più felici, poiché l'ordinaria gestione IT non rientrerebbe (nella casistica obbligatoria degli artt. 37.1.b) e 37.1.c). Ad ogni modo, il sottostante nucleo concettuale può dirsi chiaro.

Chi è tenuto a nominare il DPO?

3. Monitoraggio «regolare e sistematico»

- Ad avviso dei Garanti europei, "regolarità" non implica necessariamente "continuità". È perciò regolare anche un monitoraggio periodico, dunque discontinuo. Ciò che rileva è che sia ripetuto nel tempo (meglio se a determinati intervalli).

- «Sistematico» non va inteso in senso temporale (accezione peraltro inesistente in inglese), cosa che lo renderebbe una duplicazione di «regolare», ma in quella logica di: conforme a un sistema, a un piano, predefinito, metodico. In definitiva, non casuale né estemporaneo.

Chi è tenuto a nominare il DPO?

- Sono esempi di monitoraggio regolare e sistematico la fornitura di servizi di telefonia, la geolocalizzazione (si pensi a un'applicazione per cellulare), i programmi fedeltà, la raccolta di dati sanitari attraverso apparecchi di wellness indossabili, la videosorveglianza. In tutti questi casi, se sussiste il requisito della «larga scala» è necessaria la designazione del DPO.

Chi è tenuto a nominare il DPO?

4. «Su larga scala»

- Il Regolamento non fornisce una definizione di "trattamento su larga scala".

- Il considerando 91 fa presente che vi rientrano tra questi 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."

Chi è tenuto a nominare il DPO?

- La questione è particolarmente complessa. Sussiste un problema di quantificazione precisa, con buona pace della certezza del diritto. Basti osservare che la mancata designazione del DPO è sanzionabile ai sensi dell'art. 83.4.
- I Garanti europei ammettono l'esistenza di un'«area grigia», nella quale è incerto se possa parlarsi di attività su larga scala. Forniscono tuttavia alcuni spunti operativi utili quantomeno a limitarla.

Chi è tenuto a nominare il DPO?

- Innanzitutto non può parlarsi di larga scala nel caso di attività svolta da un professionista individuale. Il principio può essere desunto in via generale dal richiamo che i Garanti europei fanno al considerando 91.

- In altro paragrafo delle linee guida (§ 2.2) il Gruppo di lavoro mostra di considerare collocata in questa zona franca anche la «piccola impresa familiare». Si tratta per la verità di un cenno quasi incidentale, ma vista la scarsità di elementi disponibili si è tentati di farne tesoro.

Chi è tenuto a nominare il DPO?

- Più controverso il caso della «media impresa», la cui attività di trattamento potrebbe essere su larga scala a seconda del caso di specie. Lo si desume sempre da un esempio riportato al § 2.2 delle linee guida.

- Vale ora la pena notare che la nozione di PMI è precisata a livello europeo in base a parametri oggettivi indicati nella raccomandazione n. 2003/361/CE, cui l'interprete è naturalmente portato a fare riferimento.

Chi è tenuto a nominare il DPO?

Sinteticamente:

- è media impresa quella con meno di 250 dipendenti e fatturato totale annuo uguale o inferiore a 50 milioni di euro oppure un totale di bilancio annuo pari o inferiore a 43 milioni di euro;
- è piccola impresa quella con meno di 50 dipendenti e fatturato totale annuo uguale o inferiore a 10 milioni di euro oppure un totale di bilancio annuo pari o inferiore a 10 milioni di euro;

Chi è tenuto a nominare il DPO?

- è microimpresa quella con meno di 10 dipendenti e fatturato totale annuo uguale o inferiore a 2 milioni di euro oppure un totale di bilancio annuo pari o inferiore a 2 milioni di euro.

Chi è tenuto a nominare il DPO?

- Il concetto di impresa familiare (a prescindere dalle dimensioni) riposa invece, a livello europeo, su una definizione, di ampio e costante seguito, messa a punto a partire dal rapporto finale 2009 dell'Expert Group on Family Business, cui si rimanda per approfondimenti.

Chi è tenuto a nominare il DPO?

- Il collegamento del Regolamento con questi parametri dimensionali ben consolidati in ambito societario è certamente suggestivo, in quanto potrebbe aiutare a restringere i margini dell'«area grigia», tuttavia non trova supporto esplicito nelle linee guida.

Chi è tenuto a nominare il DPO?

- Queste anzi indicano criteri del tutto diversi, esclusivamente basati sul volume del trattamento anziché sulle dimensioni della struttura che vi procede. Si tratta dei seguenti:
- – numero degli interessati coinvolti dal trattamento (o percentuale della popolazione di riferimento);
- – volume dei dati personali trattati e/o loro ampiezza tipologica;

Chi è tenuto a nominare il DPO?

- – durata del trattamento;
- – contesto geografico di quest'ultimo.
- Tra gli esempi forniti di trattamento su larga scala figurano quelli di un ospedale (privato), di un'assicurazione o una banca, di un servizio di trasporto pubblico su abbonamento, di fornitori di telefonia o di servizi Internet.

Chi è tenuto a nominare il DPO?

- Ci si potrebbe domandare se una grande farmacia, un'associazione tra professionisti o uno studio medico particolarmente strutturati possano rientrare o no, a seconda dei casi, nel concetto del trattamento su larga scala.

Chi può essere nominato DPO?

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

- Il livello di conoscenza specialistica va determinato in base ai trattamenti di dati concretamente effettuati e alla protezione richiesta per i dati oggetto del trattamento.

Chi può essere nominato DPO?

- Le conoscenze e competenze specialistiche richieste alla figura del DPO includono:

- la conoscenza da parte del DPO della normativa e delle prassi, sia nazionali che europee, in materia di protezione dei dati e, in particolare, una approfondita conoscenza del Regolamento 2016/679;

- una familiarità con le operazioni di trattamento svolte;

Chi può essere nominato DPO?

- una familiarità con tecnologie informatiche e misure di sicurezza dei dati;
- la conoscenza dello specifico settore di attività e dell'organizzazione del titolare/responsabile del trattamento;
- la capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione del titolare/responsabile.

Nel caso di un'autorità pubblica o un organismo pubblico, il DPO deve possedere anche una buona conoscenza delle norme e delle procedure amministrative applicabili.

Chi può essere nominato DPO?

- Per ricoprire il ruolo di DPO il Regolamento non richiede né abilitazioni, né certificazioni, né iscrizioni ad ordini professionali. Sul punto il Garante della Privacy, con la nota 28 luglio 2017 (newsletter n. 432 del 15 settembre 2017), ha chiarito che, allo stato, le disposizioni non prevedono alcun albo dei "Responsabili della protezione dei dati", che attesti i requisiti e le caratteristiche di conoscenza, abilità e competenza, previste dal citato quadro normativo né richiedono che tali requisiti siano attestati attraverso specifiche certificazioni.

Chi può essere nominato DPO?

- Con le “Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico” il Garante della Privacy ha precisato che “come accade nei settori delle cosiddette “professioni non regolamentate”, si sono diffusi schemi proprietari di certificazione volontaria delle competenze professionali effettuate da appositi enti certificatori”.

Chi può essere nominato DPO?

- Il Garante ha ribadito categoricamente che "Tali certificazioni (che non rientrano tra quelle disciplinate dall'art. 42 del RGPD)" … "pur rappresentando, al pari di altri titoli, un valido strumento ai fini della verifica del possesso di un livello minimo di conoscenza della disciplina, tuttavia non equivalgono, di per sé, a una "abilitazione" allo svolgimento del ruolo del RPD né, allo stato, sono idonee a sostituire il giudizio rimesso alle PP.AA. nella valutazione dei requisiti necessari al RPD per svolgere i compiti previsti dall'art. 39 del RGPD".

Requisiti, indipendenza e conflitti di interesse

La figura del DPO deve avere, inoltre, le caratteristiche di indipendenza all'interno della struttura organizzativa del Titolare in cui opera, tali da consentirgli di espletare le proprie funzioni in assenza di condizionamenti dati da una preposizione gerarchica rispetto ad altri ruoli aziendali.

Secondo il Regolamento, infatti, occorre assicurare che il DPO "non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti" e riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento". Tale rapporto diretto garantisce, in particolare, che il vertice amministrativo venga a conoscenza delle indicazioni e delle raccomandazioni fornite dal DPO nell'esercizio delle funzioni di informazione e consulenza a favore del titolare o del responsabile.

Requisiti, indipendenza e conflitti di interesse

Nel caso in cui si opti per un DPO interno, è preferibile che la designazione sia conferita a un dirigente ovvero a un funzionario di alta professionalità, che possa svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione.

Il DPO, inoltre, se nominato internamente, deve ricoprire un ruolo all'interno dell'azienda tale per cui le mansioni attribuite non lo pongano in una situazione di conflitto di interessi rispetto alle responsabilità come DPO.

Analogamente a quanto avviene per la figura del *compliance officer*, il DPO non dovrà svolgere funzioni operative che comportino trattamento di dati e che, in quanto tali, rientrino nel perimetro di controllo dello stesso DPO.

Requisiti, indipendenza e conflitti di interesse

In tale prospettiva, appare preferibile evitare di assegnare il ruolo di DPO a soggetti con incarichi di alta direzione (amministratore delegato; membro del consiglio di amministrazione; direttore generale; ecc.), ovvero nell'ambito di strutture aventi potere decisionale in ordine alle finalità e alle modalità del trattamento (direzione risorse umane, direzione marketing, direzione finanziaria, responsabile IT ecc.).

Da valutare, in assenza di conflitti di interesse e in base al contesto di riferimento, l'eventuale assegnazione di tale incarico ai responsabili delle funzioni di staff (ad esempio, il responsabile della funzione legale).

Quale organo aziendale è deputato alla nomina del DPO e con quale modalità?

Il RGPD prevede all'art. 37, par. 1, che il titolare e il responsabile del trattamento designino il DPO; da ciò deriva, quindi, che l'atto di designazione è parte costitutiva dell'adempimento.

Sulla base di tale previsione, nonché in ragione del requisito di indipendenza del DPO e della relazione diretta con il vertice gerarchico del Titolare del trattamento, la nomina spetta proprio a detto vertice, da individuarsi nell'organo amministrativo di ciascuna società o ente, nelle forme deliberative previste a livello statutario.

Esaurita la fase decisionale di designazione del DPO da parte dell'organo amministrativo, il Titolare del trattamento formalizza la nomina con apposito atto.

Quale organo aziendale è deputato alla nomina del DPO e con quale modalità?

Nel caso in cui la scelta del DPO ricada su una professionalità interna all'ente, occorre formalizzare un apposito atto di nomina. In caso, invece, di ricorso a soggetti esterni all'ente, la designazione costituirà parte integrante dell'apposito contratto di servizi redatto in base a quanto previsto dall'art. 37 del GDPR.

Indipendentemente dalla natura e dalla forma dell'atto utilizzato, è necessario che nello stesso sia individuato in maniera inequivocabile il soggetto che opererà come RPD, riportandone espressamente le generalità, i compiti (eventualmente anche ulteriori a quelli previsti dall'art. 39 del GDPR) e le funzioni che questi sarà chiamato a svolgere in ausilio al titolare/responsabile del trattamento, in conformità a quanto previsto dal quadro normativo di riferimento.

Quale organo aziendale è deputato alla nomina del DPO e con quale modalità?

Nell'atto di designazione o nel contratto di servizi devono risultare succintamente indicate anche le motivazioni che hanno indotto l'ente a individuare, nella persona fisica selezionata, il proprio RPD, al fine di consentire la verifica del rispetto dei requisiti previsti dall'art. 37, par. 5 del RGPD, anche mediante rinvio agli esiti delle procedure di selezione interna o esterna effettuata.

La specificazione dei criteri utilizzati nella valutazione compiuta dall'ente nella scelta di tale figura, oltre a essere indice di trasparenza, costituisce anche elemento di valutazione del rispetto del principio di «responsabilizzazione».

Quali sono le funzioni del DPO?

L'art. 39 del Regolamento europeo sulla protezione dei dati personali elenca i principali compiti del DPO (Responsabile della protezione dei dati):

1. Il responsabile della protezione dei dati (DPO) è incaricato almeno dei seguenti compiti:

a) 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 presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

Quali sono le funzioni del DPO?

b) sorvegliare l'osservanza del presente 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;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) cooperare con l'autorità di controllo;

Quali sono le funzioni del DPO?

e) 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.

2. Nell'eseguire i propri compiti, il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Quali responsabilità possono essere imputate al DPO sotto il profilo risarcitorio, sanzionatorio e penale?

L'art. 24 par. 1 del Regolamento UE dispone "*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario*".

Quali responsabilità possono essere imputate al DPO sotto il profilo risarcitorio, sanzionatorio e penale?

Pertanto il Titolare del trattamento o il responsabile del trattamento detengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado, inoltre, di dimostrare tale osservanza.

Il rispetto delle norme in materia di protezione dei dati fa parte della responsabilità d'impresa del titolare del trattamento.

Quali responsabilità possono essere imputate al DPO sotto il profilo risarcitorio, sanzionatorio e penale?

Il DPO, sebbene incaricato di sorvegliare l'osservanza del GDPR ai sensi dell'art. 39 lett. b), non è anch'egli responsabile in caso di inosservanza del Regolamento.

In conclusione, Il *Data Protection Officer* può incorrere in responsabilità correlate allo svolgimento dei suoi obblighi di consulenza e assistenza nei confronti del titolare del trattamento, che possono essere di natura disciplinare in caso di DPO interno, o contrattuale, in caso di DPO esterno.