INDICE SOMMARIO

Capitolo IV
LA RESPONSABILITÀ DEL RESPONSABILE DELLA PROTEZIONE DATI (DATA PROTECTION OFFICER – DPO)
di Gianluca Bozzelli

Capitolo V
IL DPO IN AMBITO PUBBLICO (CORRETTO CONTROLLO): COME SCEGLIERE IL DPO IN AMBITO PUBBLICO
di Amedeo Pisanti

Capitolo VI
LA FORMALIZZAZIONE DELL'INCARICO: I CONTENUTI DELLE DELEGHE E LO SVOLGIMENTO DELLA MANSIONE
di Sara Bassolamento

Appendice
WP 29 Linee guida

Premessa

Il nuovo Regolamento europeo sulla protezione dei dati personali, divenuto legislazione comune per tutte le nazioni dell'UE, oltre ad aver introdotto nuove importanti disposizioni - ad esempio, il diritto all'oblio, alla portabilità dei dati, le notificazioni delle violazioni alle autorità nazionali e agli stessi utenti nei casi più gravi (data breach) - e regole e sanzioni più stringenti in caso di violazioni, prevede la figura del Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO).

Il DPO, figura storicamente già presente in alcune legislazioni europee, 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. La sua responsabilità principale è quella 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.

La individuazione e la successiva nomina del DPO non possono (e non devono) essere intese quali mero adempimento formale. La scelta, infatti, deve ricadere su un soggetto che sia effettivamente dotato delle qualità professionali imposte dall'art. 37 del GDPR e, 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'art. 39".

Anche se i criteri elencati nell'art. 37 del Regolamento UE 2016/679 non permettono di individuare con assoluta certezza i soggetti per i quali sarà richiesta la designazione di un DPO, in quanto vengono utilizzati concetti suscettibili di essere interpretati discrezionalmente, si può certamente affermare che il candidato DPO ideale debba possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze; egli deve poter adempiere alle sue funzioni in piena indipendenza e

in assenza di conflitti di interesse. In linea di principio, ciò significa che il DPO non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali; deve operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio (RPD/DPO esterno).

Inoltre, sempre ai sensi dell'art. 38, par. 3, del GDPR, il DPO "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.

In molti casi il Responsabile della protezione dati occupa proprio una posizione dirigenziale o manageriale stante l'obbligo di riferire al vertice gerarchico.

Il DPO potrà anche essere un dipendente dell'organizzazione oppure esterno in forza di un contratto di servizi, in quest'ultimo caso mentre l'indipendenza intesa come non ingerenza nelle proprie attività è un elemento più facile da soddisfare rispetto al DPO interno, il conflitto di interessi dovrà comunque essere disciplinato tenuto conto di alcune specificità del DPO esterno.

In ordine a quest'ultimo requisito soggettivo, il DPO interno potrà svolgere altre funzioni, ma dovrà avere sufficiente tempo per svolgere i propri compiti; a tal riguardo, sotto un profilo organizzativo si dovranno evitare situazioni di conflitto del DPO rispetto a chi gestisce processi decisionali critici dell'organizzazione in tema di protezione dei dati.

Alla luce delle considerazioni di cui sopra, nel caso in cui si opti per un DPO interno, secondo il Garante sarebbe quindi in linea di massima preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, 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.

Inoltre, alcune organizzazioni complesse hanno richiesto all'Autorità di valutare la possibilità di designare più DPO. Al riguardo, si rileva che l'unicità della figura del DPO è una condizione necessaria per evitare il rischio di sovrapposizioni o incertezze sulle responsabilità, sia con riferimento all'ambito

interno all'ente, sia con riferimento a quello esterno, e pertanto occorre che questa sia sempre assicurata.

Nulla osta, invece, all'individuazione di più figure di supporto, con riferimento a settori o ambiti territoriali diversi, anche dislocate presso diverse articolazioni organizzative dell'amministrazione, che facciano però riferimento a un unico soggetto responsabile, sia che la scelta ricada su un DPO interno, sia che questa ricada su un DPO esterno.

Infatti, in relazione alla particolare eterogeneità dei trattamenti di dati personali effettuati (in rapporto, ad esempio, all'effettuazione di trattamenti soggetti a basi giuridiche diverse in ambito di prevenzione, indagine, accertamento e perseguimento di reati) ovvero della complessità della struttura organizzativa dell'ente (talvolta molto ramificata a livello territoriale) può risultare opportuno individuare specifici "referenti" del DPO che potrebbero svolgere un ruolo di supporto e raccordo, sulla base di precise istruzioni del DPO, anche, se del caso, operando quali componenti del suo gruppo di lavoro.

Pur nella complessiva dell'istituto, appare evidente che assume rilievo la funzione di garanzia della conformità della circolazione e della protezione dei dati al Regolamento.

Napoli, 1 dicembre 2018

Commissione Privacy e Security CdO di Napoli

CAPITOLO I
IL REGOLAMENTO EUROPEO 679/2016: IL SISTEMA DEI PRINCIPI ED I SOGGETTI ATTIVI
di Marianna Quaranta

SOMMARIO: 1. Il Regolamento europeo: principi e sistematica. 2. Il Titolare del trattamento ed il responsabile del trattamento. 2.1. *Data protection by default and by design.* 3. La figura del Data Protection Officer (DPO)

1. Il Regolamento europeo: principi e sistematica

Come ormai noto, il 27 aprile 2016 la Commissione Europea ha presentato un Regolamento per l'aggiornamento della normativa concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati. (d'ora innanzi anche GDPR)[1]

Il Regolamento UE, essendo un atto *self executive*, ai sensi dell'articolo 288 del Trattato sul Funzionamento dell'Unione Europea, è direttamente esecutivo e non necessita di recepimento da parte degli Stati membri, cosicché a decorrere dal 25 maggio 2018, la normativa su citata è diventata immediatamente applicabile anche nello Stato italiano.

È, altresì, noto che la legge 675/1996 ed il D.Lgs. 196/2003, come da ultimo emendato ai fini dell'adeguamento al GDPR dal D.Lgs.108/2018, costituiscono le pietre miliari che hanno posto le fondamenta della normazione del diritto alla "privatezza" individuando, in capo al titolare del trattamento, un sistema di adempimenti che consentisse, una volta applicato, di ritenere correttamente eseguito il trattamento dei dati.

In particolare, l'impianto normativo disegnato dal Codice della Privacy consentiva di individuare, con un sufficiente grado di dettaglio, le misure di sicurezza che, secondo il legislatore, potevano considerarsi "necessarie e sufficienti" ai fini della correttezza del trattamento. Segnatamente, l'allegato B del citato D.Lgs.196/2003 prevedeva per l'appunto la regolamentazione e l'elencazione delle misure minime di sicurezza da applicare, specie con riferimento ai trattamenti di tipo telematico e informatico.

[1] F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, G. Giappichelli Editore, Torino 2016, pp. 38, 39.

Di qui la previsione di un documento programmatico sulla sicurezza (DPS) la cui adozione ed aggiornamento non solo erano obbligatori, ma anche suscettibili di sanzione sia in sede civile che penale.

Il superamento della obbligatorietà di talune misure sembrava declinare un sistema che alleggerisse il titolare del trattamento, in realtà, il nuovo Regolamento Europeo è impostato sul principio cosiddetto dell'*accountability*[2], ovvero, la normativa stabilisce che sia il titolare del trattamento ad individuare quelle misure che possano, in maniera adeguata, tutelare gli interessati al trattamento.

Questa impostazione sbilancia fortemente l'asse a carico del titolare del trattamento il quale se, da un lato, sembra alleggerito del sistema degli adempimenti, dall'altro, proprio per la valutazione di congruità a lui rimessa del sistema adottato, impone una *risk analysis* che deve essere eseguita, onde individuare quelle criticità nella *governance* del trattamento dei dati che potrebbero determinare lesioni dei diritti dell'interessato.

Ma procediamo con ordine.

2. Il Titolare del trattamento ed il responsabile del trattamento.

Se questo per i temi che qui interessano è il principio cardine, il Regolamento non manca di intervenire sui soggetti che, dal lato attivo, presiedono al trattamento.

In particolare, si è già detto, che con il sistema dell'*accountability* il regime delle responsabilità si sbilancia fortemente a carico del titolare del trattamento, il quale se, da un lato, può individuare, in base al tipo di trattamento eseguito e alla sua struttura, le migliori modalità per l'esecuzione del trattamento e la raccolta del dato, dall'altro, deve preoccuparsi di dimostrare di aver adottato misure sufficienti sotto il profilo tecnico ed organizzativo, adeguate a consentire il rispetto dei diritti dell'interessato.

Un supporto significativo, in tal senso, viene offerto dal responsabile del trattamento il quale dovrà essere incaricato dal titolare che dovrà darsi carico di specificare, in maniera chiara, i compiti specifici attribuitigli. Nel far ciò, il titolare del trattamento dovrà preoccuparsi di fornire tutte le indicazioni e le

[2] M. J. DUBNICK, *Accountability and the Promise of Performance: In Search of the Mechanisms*, Public Performance and Management Review, vol. 28, n. 3, 2005.

prescrizioni che il responsabile del trattamento dovrà porre in essere. In particolare, attraverso un contratto o altro atto giuridico conforme al diritto nazionale, il titolare del trattamento dovrà preoccuparsi di evidenziare, oltre alle istruzioni e alle misure tecniche ed organizzative adeguate a consentirne il rispetto, anche di specificare la natura, la durata e la finalità del trattamento o dei trattamenti, anche diversi, eventualmente assegnati al responsabile.

È possibile, diversamente da quanto previsto per il passato, che vi sia la nomina da parte del responsabile del trattamento, di sub - responsabili per specifiche attività sempre che tale (sub) nomina avvenga nel rispetto degli obblighi contrattuali dal primo assunti.

Questi risponderà, dinanzi al titolare, dell'eventuale inadempimento del sub - responsabile anche ai fini del risarcimento di eventuali danni, a meno che non dimostri che l'evento dannoso non gli è in alcun modo, imputabile.

I responsabili del trattamento, ai sensi dell'articolo 30, del Regolamento in commento sono tenuti a predisporre il registro delle attività di trattamento eseguite; essi devono, altresì, provvedere all'adozione di idonee misure tecniche ed organizzative, onde garantire la sicurezza dei trattamenti. Il responsabile del trattamento dovrà, altresì, preoccuparsi di impartire le dovute istruzioni agli incaricati al trattamento, ovvero, a coloro che materialmente eseguono il trattamento, seguendo le prescrizioni impartite dal titolare e dal suo responsabile.

Invero, la normativa europea non prevede, in maniera espressa, la figura dell'incaricato al trattamento, così come avveniva per il Codice, ma non ne esclude la presenza, in quanto, fa riferimento a persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

In altri termini, implicitamente riconosce queste figure per le quali, in mancanza di diverse prescrizioni, possono valere le indicazioni già previste dal Codice.

Per agevolare il compito non semplice del titolare del trattamento e del suo responsabile di dare atto di aver adottato misure adeguate, il Regolamento prevede l'adesione a codici deontologici, ovvero, l'adesione a schemi di certificazione che possano aiutare il responsabile del trattamento a dimostrare di aver adottato le cautele per eseguire, in sicurezza, il trattamento affidatogli. Allo stato, il Garante sta valutando la diffusività dei codici, già attualmente vigenti per alcune tipologie

di trattamento, rivisti alla luce dei requisiti fissati dal Regolamento all'articolo 40, mentre, non vi sono ancora "schemi di certificazione" (Art. 42) per i quali occorre l'intervento del legislatore che dovrà stabilire le modalità di accreditamento dei soggetti certificatori.

La responsabilizzazione dei titolari e dei responsabili del trattamento poggia sull'adozione di comportamenti proattivi che dimostrino la concreta applicazione delle misure finalizzate ad assicurare la corretta attuazione del regolamento.

Si tratta di una rivoluzione copernicana che ribalta sul titolare del trattamento la scelta delle modalità ritenute più idonee a garantire un trattamento efficace e sicuro.

2.1. *Data protection by default and by design*

Tra i criteri che il Regolamento ha sintetizzato, a vantaggio del titolare, il primo è quello di cui all'articolo 25, dove si fa riferimento al cosiddetto *data protection by default and by design*, ossia, alla necessità di configurare il trattamento, prevedendo, fin dall'inizio, le garanzie indispensabili al fine di tutelare, in maniera adeguata, i diritti degli interessati, tenendo conto del contesto complessivo in cui il trattamento si colloca e dei rischi che esso pone alla libertà e ai diritti degli interessati nel rispetto di quanto sancito dal GDPR.

Le scelte effettuate dal titolare devono essere fatte a monte e, pertanto, si richiede un'analisi preventiva ed un impegno applicativo da parte di titolari che devono darsi carico della predisposizione di attività specifiche e dimostrabili.

Nella valutazione dei rischi, il titolare del trattamento dovrà valutare l'impatto negativo che il medesimo ha sulle libertà e sui diritti degli interessati, secondo quanto previsto ai considerando 75 e 77 del Regolamento, naturalmente, tale impatto dovrà essere analizzato attraverso un idoneo processo di valutazione, la cosiddetta *Risk Analysis* descritto agli articoli 35 e 36.

Tale processo di valutazione dovrà tener conto dei rischi noti o di quelli ipotizzabili ed evidenziabili con la conseguente adozione di misure di sicurezza tecniche e organizzative che consentano di mitigare tali rischi.

All'esito della valutazione dei rischi, il titolare potrà decidere in autonomia se iniziare il trattamento, ritenendo, in tal caso, di aver adottato tutte le misure di

sicurezza necessarie e sufficienti a mitigare gli effetti dei rischi, ovvero, potrà, in via preventiva, consultare il Garante per la protezione dei dati personali, onde, ottenere indicazioni su come gestire il rischio residuale.

In tal caso, l'Autorità non avrà il compito di autorizzare il trattamento, ma di indicare eventuali ulteriori misure correttive da adottare. In altri termini, l'Autorità interverrà principalmente ex post e ciò spiega perché, a partire dal 25 maggio 2018, alcuni istituti come, ad esempio, quello della notifica di taluni trattamenti, ovvero, la verifica preliminare di taluni altri di cui all'articolo 17 del Codice, sono superati a vantaggio degli obblighi di tenuta del registro dei trattamenti da parte del titolare e del responsabile del trattamento.

In ogni caso, è fatto obbligo a tutti i titolari e responsabili di trattamento, eccetto gli organismi con meno di 250 dipendenti e sempre che non effettuino trattamenti a rischio, di tenere un registro delle operazioni di trattamento i cui contenuti sono specificati all'articolo 30 del GDPR.

Si tratta di uno strumento che consente di predisporre all'interno dell'azienda, di un quadro aggiornato dei trattamenti in corso ed è indispensabile per ogni valutazione ed analisi del rischio.

Il registro può avere forma scritta anche elettronica e deve essere esibito su richiesta del Garante, ovvero, dei suoi ausiliari, consentendo all'Autorità di supervisionare il trattamento e verificarne la compatibilità con il Regolamento.

Per quel che concerne i contenuti, l'articolo 30 prevede che nel registro siano annotate una serie di informazioni: in particolare, deve essere specificato il nome ed i dati di contatto del titolare del trattamento e ove previsto del rappresentante del titolare del trattamento e del responsabile della protezione dei dati.

Vanno specificate le finalità del trattamento e descritte le categorie di interessati e dei dati personali trattati, nonché, le categorie di destinatari a cui dati sono stati o saranno comunicati, compresi i destinatari di paesi terzi o le organizzazioni internazionali. Se vi è un trasferimento di dati verso un paese terzo o un'organizzazione internazionale deve esserle data indicazione nel predetto registro compresa l'identificazione del paese terzo o l'organizzazione internazionale verso cui il dato viene trasmesso. Naturalmente, si dovrà dare atto nel medesimo registro di aver adottato garanzie adeguate, suffragando le attività

con idonea documentazione; infine, dovranno essere indicati, laddove sia possibile, i termini previsti per la cancellazione dei dati e una descrizione generale delle misure di sicurezza tecniche ed organizzative adottate.

La tenuta del registro non costituisce un adempimento formale, ma al contrario esso costituisce parte integrante di un sistema di corretta gestione del dato personale, pertanto, i titolari del trattamento ed i responsabili, a prescindere dalle dimensioni dell'organizzazione, devono compiere i passi necessari per dotarsi di tale registro ed, in ogni caso, occorre compiere un'accurata ricognizione dei trattamenti per verificarne la compatibilità con il Regolamento.

3. La figura del Data Protection Officer (DPO)

Il completamento naturale del nuovo impianto normativo, potremmo dire, si sintetizza nella previsione di un responsabile della protezione dei dati, meglio noto come *Data Protection Officer* (DPO). Si tratta di una nuova figura professionale che il Regolamento prevede sia adottata obbligatoriamente per alcune categorie di soggetti e con riferimento a talune tipologie di trattamento.

Compito precipuo del DPO è la sensibilizzazione e la formazione del personale, nonché, la sorveglianza sullo svolgimento della valutazione di impatto del trattamento, secondo quanto previsto dall'articolo 35 del Regolamento.

Si tratta di una figura professionale che si caratterizza per indipendenza, autorevolezza e competenze manageriali. In particolare, l'articolo 37 ne prevede la nomina in tre casi specifici: a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico; b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; c) se le attività principali del titolare o del responsabile e consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati. La novità di tale figura professionale e la mancanza, allo stato, nel nostro sistema giuridico di prescrizioni qualificanti che si auspica provengano dal Garante per la protezione dei dati personali in tempi rapidi, consente di avere come unico riferimento le linee guida adottate dal Gruppo di lavoro ex art. 29 cui si rinvia per gli opportuni approfondimenti, in questa sede, val la pena sottolineare che, a prescindere dalla

nomina di un DPO, è fortemente raccomandato ai titolari ed ai responsabili del trattamento di documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se, nel caso specifico, sia o meno d'obbligo provvedere alla nomina di un DPO, in modo da dare atto che la *risk analysis* ha preso in esatta considerazione i fattori pertinenti. Se si procede alla nomina di un DPO su base volontaria, naturalmente, varranno per il medesimo le stesse prescrizioni previste per il caso di nomina obbligatoria.

Le conoscenze e le competenze del DPO consistono, prevalentemente, nella conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché, nella capacità di assolvere ai compiti al medesimo assegnati dall'articolo 39 del Regolamento: se nominato devono essere messi a disposizione degli interessati anche i riferimenti, ovvero, i dati di contatto del DPO.

Questa figura professionale risulta essere preziosa per il titolare non solo quando l'attività sia già avviata, ma, anche e soprattutto, nelle fasi iniziali in merito alla valutazione dei rischi atteso che uno dei compiti del DPO è proprio quello di informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, nonché, agli incaricati al trattamento che lo eseguono.

Queste, in estrema sintesi, le direttrici del nuovo Regolamento sui soggetti attivi del trattamento che impongono di provvedere ai necessari adeguamenti.

Tale obbligo prescinde, se non per le specificità evidenziate, dalle dimensioni dell'impresa ed impone a tutti i titolari del trattamento l'adeguamento, stante il superamento, in *parte qua*, di quanto previsto dal Codice della Privacy come emendato dal nuovo D.Lgs.101/2018, soprattutto, in vista dell'aggravamento del sistema delle responsabilità in capo al titolare del trattamento e dell'imponente sistema sanzionatorio connesso. In questo contesto, la figura del DPO assume un ruolo pregnante e, come meglio si leggerà nei prossimi contributi, si presta a svolgere una funzione di controllo e di garanzia sia nell'attuazione della normativa che nella gestione aziendale nel contesto privato che pubblico.

CAPITOLO II

IL D.P.O. COME CONSULENTE DELL'ATTIVITA' DI RISK ANALYSIS. RAPPORTI CON LE FUNZIONI AZIENDALI

di Sergio Falcone

SOMMARIO: 1. I principi generali. 2. Il DPO all'interno dell'organizzazione. 2.1. L'indipendenza del DPO. 3. La Risk Analysis nel GDPR. 3.1. I principi generali. 3.2. Il ruolo del DPO nell'analisi del rischio. 4. Il DPO e la gestione del rischio. 4.1. Il risk management. 4.2. La valutazione del rischio. 4.3. Il registro dei trattamenti. 4.4. La Dpia. 4.5. La sicurezza dei trattamenti.

1. I principi generali

Il GDPR attribuisce un ruolo fondamentale all'analisi del rischio derivante dal trattamento dei dati personali. Il principio cardine dello stesso Regolamento, quell'*accountability* tradotto nel più ampio concetto di responsabilizzazione, si impersonifica in tale contesto nella figura del DPO quale Responsabile della Protezione dei Dati (RPD). Egli si configura come soggetto di consulenza designato all'interno dell'ente/azienda, e quindi di supporto al titolare del trattamento nello svolgimento dell'insieme di procedure necessarie per la protezione dei dati personali trattati.

Sappiamo, difatti, che spetta proprio al titolare mettere "in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento" (art. 24, comma 1 GDPR). In virtù di tale dettato, rientra tra gli obblighi del titolare, e non del DPO, quello relativo alla tenuta del registro dei trattamenti (art. 30, comma 1 GDPR) e allo svolgimento di una valutazione di impatto sulla protezione dei dati, la DPIA (art. 35, comma 1, GDPR).

L'art. 39 del Regolamento elenca genericamente i compiti del DPO, specificando al comma 1 la natura di informazione e consulenza del suo operato a favore del titolare del trattamento e degli altri soggetti all'interno dell'ente/azienda, così come di parere sulla valutazione di impatto sulla protezione dei dati.

Il WP29 è intervenuto in realtà con il parere del 13 dicembre 2016 per colmare la mancanza, all'interno del Regolamento, di specifiche indicazioni in merito alle

mansioni attribuite al DPO, stabilendo, tra l'altro, il principio secondo il quale è nelle facoltà del titolare delegare al responsabile del trattamento dei dati la tenuta del registro, oggetto peraltro necessario a quest'ultimo per una corretta pianificazione del *risk management.*

2. Il DPO all'interno dell'organizzazione

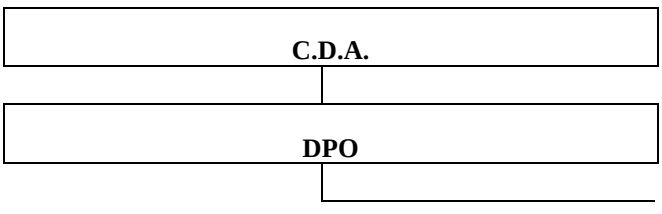
Il legislatore europeo delinea in maniera chiara la figura del responsabile della protezione dei dati quale supervisore indipendente incaricato formalmente dai soggetti apicali di aziende pubbliche o private per la salvaguardia del rispetto della tutela dei dati personali trattati.

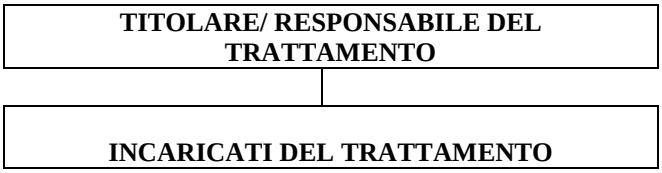
Al DPO viene riconosciuto un ruolo di fatto pervasivo, giacché è previsto un suo diretto e tempestivo coinvolgimento su ogni questione legata alla garanzia della protezione dei dati personali trattati, e dovendo a tal fine supervisionare tutte le attività di attribuzioni dei ruoli e responsabilità all'interno dell'ente/azienda, i piani di sensibilizzazione, di formazione nonché le attività di controllo sulle procedure, come ad esempio quello di adeguatezza dei piani di audit interno.

L'art. 37, comma 6 GDPR stabilisce che "il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi".

Basilare è la rispondenza della figura del DPO designato al requisito di assenza di conflitto di interesse nello svolgimento delle sue mansioni nell'ente/azienda, ragione per la quale egli non può in alcun modo intervenire nella scelta delle finalità o degli strumenti necessari allo svolgimento dei trattamenti dei dati.

Il DPO deve, quindi, poter svolgere la propria attività in piena e totale indipendenza, collocandosi di fatto, all'interno dell'organigramma aziendale, in una posizione autonoma ed intermedia tra i soggetti apicali e il titolare del trattamento.





L'art. 38, comma 1 GDPR prevede, inoltre, che "il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali". Ciò comporta la necessità di un suo coinvolgimento ogni qualvolta si profili la possibilità di dover procedere alla definizione di nuovi trattamenti o di modifica nella modalità di svolgimento di quelli già esistenti, nel rispetto del principio della protezione dei dati fin dalla progettazione (*privacy by design*).

2.1. L'indipendenza del DPO

L'art. 38, comma 3, definisce le garanzie necessarie al DPO per il corretto svolgimento delle sue mansioni: "il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento".

Laddove, il titolare o il rappresentante del trattamento non seguissero i dettati del GDPR o le indicazioni del DPO, quest'ultimo non solo dovrebbe godere della possibilità di mostrare il proprio dissenso ai vertici apicali dell'ente/azienda ma anche di vedersi riconosciuta una adeguata tutela dalla minaccia di possibile rimozione o penalizzazione per l'adempimento dei propri compiti.

In ogni caso, quindi, il DPO non può essere rimosso o penalizzato dal titolare o dal responsabile del trattamento per l'adempimento dei propri compiti in ossequio al GDPR.

Le linee guida del WP29 stabiliscono, tra l'altro, che nell'adempimento delle sue mansioni egli debba essere dotato di personale, locali e attrezzature sufficienti per

adempiere i propri compiti, in misura proporzionale alle dimensioni dell'ente/azienda e dei trattamenti da questa effettuati. Le linee guida prevedono inoltre che dovrà essere messa a sua disposizione una linea di budget adeguata alla complessità dell'organizzazione.

3. La Risk Analysis nel GDPR

Il cambio di approccio nei confronti della gestione della privacy contenuta nel GDPR impone una rivisitazione nella progettazione e modalità di esecuzione dell'analisi del rischio relativa al trattamento di dati personali. I principi della *Privacy by Design* e della *Privacy by Default*, così ben enunciati nell'art. 25 e tradotti come processi di "protezione dei dati fin dalla progettazione e protezione per impostazione predefinita", comportano senza dubbio una serie di nuove implicazioni a livello gestionale ed organizzativo all'interno dell'ente/azienda. L'approccio proattivo, e quindi non più reattivo, stabilito dal legislatore europeo conferisce ancor più importanza allo strumento dell'analisi del rischio, chiamato a dimostrare l'adeguatezza delle misure implementate dal titolare del trattamento a tutela dei dati trattati, e a riprova del principio di *accountability* del quale egli stesso è chiamato a rispondere.

Al titolare spetta, difatti, l'onere di dimostrare con quali modalità ha provveduto alla protezione dei dati e quali sono i rischi che corrono gli interessati dal momento in cui ne autorizzano il loro trattamento.

3.1. I principi generali

La gestione dei rischi in ambito privacy si traduce nell'insieme di attività volte ad indirizzare e controllare un'organizzazione in relazione ai rischi sui trattamenti dei dati personali.

L'art. 32, comma 2, del GDPR stabilisce che "nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati", evidenziando di fatto quei rischi che il titolare dovrà proattivamente evitare che si verifichino all'interno

della realtà aziendale.

Il Regolamento richiama la valutazione dei rischi attraverso due modalità:

1 – una valutazione dei rischi per i diritti e le libertà delle persone fisiche ex artt. 24, 25 e 32 GDPR

2 – una valutazione di impatto sulla protezione dei dati (DPIA) ex art. 35 GDPR

3.2. Il ruolo del DPO nell'analisi del rischio

L'attività di analisi del rischio richiede una preparazione adeguata in tema privacy non solo in campo normativo, ma anche a livello organizzativo, procedurale e tecnico.

In tale contesto, la figura del DPO riveste una posizione chiave all'interno del GDPR: la sua conoscenza sulle modalità di valutazione e gestione dei rischi, unitamente alla conoscenza degli standard di gestione in ambito privacy, lo rendono più che mai indispensabile all'interno dell'ente/azienda, tanto che il WP29 suggerisce di nominare un responsabile per la protezione dei dati anche in assenza di obbligo specifico. Egli può difatti garantire una più rapida ed efficace analisi dei rischi, ottimizzando i costi di gestione e soprattutto allineando la *risk analysis* agli standard previsti dalle normative.

4. Il DPO e la gestione del rischio

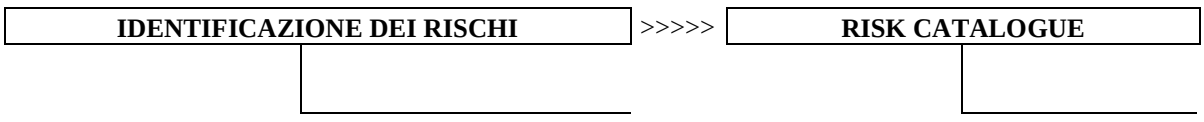
4.1. Il risk management

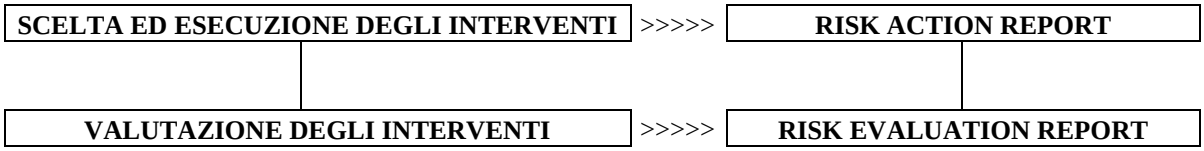
La gestione del rischio, o *risk management*, permette di prevenire e quindi evitare la possibilità di violazione dei dati personali trattati all'interno dell'ente/azienda. Sintetizzando e semplificando tale insieme di operazioni, potremmo definire ex ante 3 imprescindibile tappe:

1 – la previsione dei possibili eventi negativi nel trattamento dei dati

2 – la progettazione e realizzazione di un piano di sicurezza idoneo

3 – la valutazione del piano elaborato





Le fasi sopra descritte vanno considerate all'interno di un processo dinamico di tipo circolare: laddove la valutazione sull'efficacia degli interventi dovesse risultare negativa, si dovrà tornare ad una nuova e più esaustiva identificazione dei rischi e ad una loro quantificazione (nuova *risk catalogue*) e quindi alla progettazione di nuove strategie (*risk action report*).

La gestione dei rischi deve contestualmente prevedere, come stabilito dal GDPR, modalità operative distinte basate sulla minaccia di rischio potenziale o di rischio effettivo, e condizionate dal grado di rischio stesso a cui è sottoposto il trattamento:

	RISCHIO POTENZIALE (PRIMA DEL TRATTAMENTO)	**RISCHIO EFFETTIVO (DURANTE IL TRATTAMENTO)**
TRATTAMENTI DI DATI PERSONALI	**ANALISI DEL RISCHIO ex art. 25 GDPR (privacy by design/default)**	**AGGIORNAMENTO PERIODICO DELL'ANALISI ex art. 32 GDPR (sicurezza del trattamento)**
TRATTAMENTI AD ALTO RISCHIO	**DPIA ex art. 35 GDPR (valutazione di impatto)**	**DPIA ex art. 35 comma 11 GDPR (riesame del trattamento già sottoposto a DPIA)**

4.2. La valutazione del rischio

Fondamentale per una corretta ed efficace *risk analysis* è senza dubbio la scelta della modalità di valutazione, e quindi classificazione, dei rischi. In tale contesto il GDPR non fornisce indicazioni specifiche, ma possiamo attingere modelli di valutazione dei rischi dalle linee guida e dalle raccomandazioni del Garante per la Privacy, del WP29, o di fonti autorevoli quali agenzie e organismi di certificazione.

I rischi così individuati vanno valorizzati, e a tal fine ciascuna organizzazione può liberamente avvalersi di un proprio modello per categorizzare e misurare i rischi (modelli qualitativi, quantitativi, misti).

Adottiamo a titolo esemplificativo un modello estremamente semplice e lineare.

Punto di partenza è la valutazione del "Rischio Potenziale Lordo", ossia del rischio al lordo delle misure di sicurezza applicate. È necessario, quindi, individuare tipologia e quantità di dati oggetto del singolo trattamento, e successivamente definire, per ogni trattamento, i rischi potenziali che deriverebbero dalla perdita di sicurezza dei dati.

RISCHIO = IMPATTO X PROBABILITA'

IMPATTO							
	MOLTO ALTO		**5**	**10**	**15**	**20**	**25**
	ALTO		**4**	**8**	**12**	**16**	**20**
	MEDIO		**3**	**6**	**9**	**12**	**15**
	BASSO		**2**	**4**	**6**	**8**	**10**
	MOLTO BASSO		**1**	**2**	**3**	**4**	**5**
			MOLTO BASSO	**BASSO**	**MEDIO**	**ALTO**	**MOLTO ALTO**

PROBABILITA'

Stabilito il valore lordo del rischio, è possibile individuare all'interno del registro tutti quei trattamenti che presentano alti indici di rischio, e quindi di criticità.

Applicando idonee misure di sicurezza si addiverrà alla riduzione della probabilità di rischio di violazione dei dati.

Il "Rischio Effettivo Netto" verrà così calcolato con la stessa matrice e rappresenterà il valore del rischio ridotto, quindi al netto delle misure di sicurezza applicate. La riduzione di tale valore rappresenterà la validità delle misure intraprese a tutela della salvaguardia dei dati trattati, e ciò sarà maggiormente vero laddove le misure stesse risponderanno all'esigenza di efficacia e saranno soggette a costante verifica e monitoraggio.

Il posizionamento del valore del "rischio netto" all'interno delle diverse zone della matrice determinerà la seguente valutazione del rischio:

- verde = valore accettabile

- giallo = necessità di interventi di mitigazione
- arancio/rosso = necessità immediata di contromisure

A questo punto non resterà che definire le soluzioni tecniche e organizzative necessarie ad una tempestiva riduzione dei rischi.

4.3. Il registro dei trattamenti

Il registro dei trattamenti rappresenta il primo e necessario adempimento in ambito di *risk management*. Il registro permette, infatti, di disporre di un quadro aggiornato dei trattamenti posti in essere all'interno dell'ente/azienda, rendendolo di fatto uno strumento imprescindibile al fine di una corretta analisi dei rischi. L'art. 30 del GDPR stabilisce le casistiche per le quali la tenuta del registro rappresenta un obbligo (ente/azienda con più di 250 dipendenti, …), ma senza dubbio è altamente consigliato predisporne uno per facilitare lo svolgimento di una corretta *risk analysis*.

Il registro dovrà contenere le seguenti informazioni:

- il nome e i dati di contatto del titolare, e ove applicabile del responsabile e del DPO
- l'area aziendale in cui i dati vengono trattati
- gli interessati
- le finalità del trattamento
- le categorie di dati trattati
- le categorie di destinatari
- se è previsto o meno il trasferimento di dati verso un Paese terzo, soprattutto se extra UE
- il termine ultimo stabilito per la cancellazione dei dati
- gli strumenti del trattamento
- la sicurezza del trattamento stesso

Attraverso la redazione e l'aggiornamento del registro è possibile quindi impostare fin dalle prime fasi un adeguato approccio alla sicurezza, non tralasciando l'altra importante funzione del registro, ossia quella di dimostrazione della conformità della gestione privacy dell'ente/azienda ai dettati del GDPR in caso di verifica da parte dell'Autorità di controllo.

4.4. La DPIA

L'art. 35 del GDPR disciplina un importante ed innovativo strumento di tutela della privacy, la valutazione di impatto sul trattamento dei dati, la DPIA (*Data Protection Impact Assessment*), richiesta laddove il trattamento presenti un rischio elevato per gli interessati.

La DPIA si configura come un processo in grado di valutare la liceità, necessità e proporzionalità del trattamento, e di valutare e gestire i rischi per i diritti e le libertà delle persone fisiche i cui dati personali sono trattati. Laddove un trattamento evidenzi la possibilità di un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento ha difatti l'obbligo di effettuare una DPIA, consultando il DPO laddove ne sia stato designato uno.

Il WP29 ha pubblicato il 4 aprile 2017 un documento contenente le linee guida per lo svolgimento della valutazione di impatto, chiarendo il concetto espresso dal GDPR al comma 1 dell'articolo 35. In particolare, il riferimento a "diritti e libertà" degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la libertà di parola, di pensiero, di coscienza, di religione e di circolazione. Laddove, si instauri il dubbio se una situazione richieda o meno lo svolgimento della DPIA, la raccomandazione del WP29 è quella di effettuarlo a prescindere, in quanto strumento utile e idoneo per il rispetto della legge in materia di protezione dei dati.

La DPIA è richiesta nello specifico (art. 35, comma 3 GDPR):

- laddove si proceda ad una "valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basate su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche";
- nel caso di "trattamento, su larga scala, di categorie particolari di cui all'articolo 9, paragrafo 1, o i dati relativi a condanne penali e ai reati di cui all'art. 10" (cd. dati sensibili e dati relativi a condanne penali e reati);

- nel caso di “sorveglianza sistematica su larga scala di una zona accessibile al pubblico”.

Si aggiungano, su indicazione del Garante Privacy, i casi in cui:

- si utilizzino dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ...);
- si proceda all’applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale)
- si eseguano trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

Il WP29 ritiene invece che la DPIA non sia richiesta nei seguenti casi:

- laddove, il trattamento non presenti un “rischio elevato per i diritti e le libertà delle persone fisiche”
- laddove, le caratteristiche di un trattamento (contesto, finalità, natura ed ambito di applicazione) siano del tutto simili a quelle di un trattamento per il quale è già stata effettuata una DPIA

A livello operativo, anche in questo caso numerosi sono i modelli disponibili per la valutazione quantitativa e qualitativa dell’impatto sui dati trattati, tra questi la matrice riportata nel paragrafo precedente per la valutazione del grado di rischio di un trattamento di dati personali.

4.5. La sicurezza dei trattamenti

L’art. 32 del GDPR indica le “misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio” a carico del titolare e del responsabile del trattamento:

- la pseudonimizzazione e la cifratura dei dati personali
- la capacità di assicurare la riservatezza, l’integrità, la disponibilità dei dati e la resilienza dei sistemi
- la capacità di ripristinare tempestivamente la disponibilità e l’accesso dei dati personali in caso di incidente fisico o tecnico

- una procedura per verificare, testare e valutare regolarmente l'efficacia delle misure tecniche e organizzative

Spetta al titolare del trattamento, coadiuvato dal DPO, effettuare idonee e preventive valutazioni di impatto privacy sui trattamenti dei dati e, di conseguenza, implementare specifiche ed adeguate misure di sicurezza. Ciò si traduce in un vero e proprio cambio di approccio alla gestione del rischio da parte del Regolamento europeo rispetto al Codice Privacy preesistente: laddove quest'ultimo si limitava ad indicare i requisiti minimi richiesti da un sistema di sicurezza, il GDPR delega totalmente al titolare del trattamento la definizione di misure idonee ed adeguate al caso specifico. Recita inoltre l'art. 32 del GDPR al comma 3 che "l'adesione a un codice di condotta… o a un meccanismo di certificazione… può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo", rimarcando l'importanza di tali strumenti per una corretta ed idonea salvaguardia dei dati personali trattati.

CAPITOLO III

MANSIONI DATA PROTECTION OFFICER (D.P.O,)

di Alessandro Varriale

SOMMARIO: 1. Regolamento sulla protezione dei dati personali UE 2016/679. 2. Data Protection Officer (DPO) - Mansioni

1. Regolamento sulla protezione dei dati personali UE 2016/679

Il Regolamento Europeo per la protezione dei dati personali 679/2016 (Regolamento o GDPR) come noto, obbligatorio in tutti i Paesi membri dell'unione Europea a partire dal 25 maggio u.s., raccoglie l'esperienza maturata in Europa negli ultimi venti anni, proponendosi di armonizzare la disciplina della privacy a livello comunitario, nell'ottica di individuare un'unica norma uniforme quale minimo comune denominatore fra i 28 Stati membri.[3] Proprio nel solco di tale principio, l'Italia, come detto, con il decreto legislativo di armonizzazione del 10 agosto 2018 n.101, pubblicato in Gazzetta Ufficiale il 4 settembre 2018, ha emendato il d.lgs. n°196/03 (Codice Privacy). Il GDPR nasce da precise esigenze, come indicato dalla stessa Commissione Ue, di certezza giuridica, armonizzazione e maggiore semplicità delle norme riguardanti il trasferimento di dati personali dall'Ue verso altre parti del mondo. Si tratta poi di una risposta, necessaria e urgente, alle sfide poste dagli sviluppi tecnologici[4], e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali sempre più avvertite dai cittadini Ue. A preoccupare sono, però, le disposizioni di *ratio* sostanzialmente opposte che hanno attribuito agli Stati membri la possibilità di legiferare in autonomia al fine di "precisare" le norme contenute nel GDPR. In qualche modo si è tradita l'iniziale visione dell'Ue e potrebbero sorgere contrasti tra il Regolamento e le leggi nazionali adottate per allinearsi alle nuove indicazioni.

---

[3] Nota bibliografica, G. CASSANO, *Guida informativa sul Regolamento sulla protezione dei dati personali UE 2016/679*; *Sale For Human Resources Consulting* - Appunti Corso alta formazione manageriale DPO 25/01/18; Garante per la protezione dati personale – Il Responsabile della protezione dati; Garante per la protezione dati personale – Codice Privacy. Tribunale Amministrativo Regionale Friuli Venezia Giulia – Sent. n°287/18 del 13 settembre 2018.

[4] A inizio ottobre il WP29 ha adottato tre fondamentali provvedimenti che avranno importanti ricadute su punti essenziali del GDPR proprio sul tema dell'innovazione tecnologica.

In estrema sintesi col GDPR vengono: (i) introdotte regole più chiare su informativa e consenso; (ii) definiti i limiti al trattamento automatizzato dei dati personali; (iii) Poste le basi per l'esercizio di nuovi diritti; (iv) Stabiliti criteri rigorosi per il trasferimento degli stessi al di fuori dell'Ue; (v) Fissate norme rigorose per i casi di violazione dei dati (*data breach*).

Le norme si applicano anche alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti all'interno del mercato Ue. Tutte le aziende, ovunque stabilite, dovranno quindi rispettare le nuove regole. Imprese ed Enti avranno più responsabilità e caso di inosservanza delle regole rischiano pesanti sanzioni.

Per risolvere eventuali difficoltà è stato introdotto lo "sportello unico" (*one stop shop*), che semplificherà la gestione dei trattamenti e garantirà un approccio uniforme. Le imprese che operano in più Stati Ue potranno rivolgersi al Garante Privacy del Paese dove hanno la loro sede principale. In realtà, almeno in Italia, oltre la metà delle aziende – ma anche tante Pubbliche Amministrazioni – non è ancora pronta ad allinearsi ai provvedimenti Ue in materia di *data protection* nonostante le severe sanzioni previste.

Un aiuto potrebbe arrivare dal Piano Industria che permetterebbe di investire per avviare l'adeguamento al GDPR. Il Garante ha dato precise indicazioni alle PA. Le priorità operative sono tre:

1. La designazione in tempi stretti del Responsabile della protezione dei dati;
2. L'istituzione del Registro delle attività di trattamento;
3. La notifica dei *data breach*.

Per *data breach*, nella versione italiana, violazione dei dati personali, si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Sempre secondo il GDPR, la notifica di eventuali violazioni di dati dovrà avvenire possibilmente senza ingiustificato ritardo e, ove possibile, entro 72 ore, dal momento in cui si è venuto a conoscenza della violazione, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. L'eventuale ritardo dovrà essere motivato. Il titolare del trattamento dovrà comunicare eventuali violazioni dei dati personali al Garante.

Rispondere in modo efficace a un *data breach* per il GDPR, richiede un approccio multidisciplinare ed integrato e una maggiore cooperazione a livello Ue. L'attuale approccio presenta numerose falle che vanno corrette.

Non è semplice ma occorre farlo per non perdere l'occasione fornita dal GDPR. Il primo adempimento da porre in essere per le imprese italiane è senz'altro l'adozione del Registro dei trattamenti di dati personali, ma prima ancora che delle beghe burocratiche, l'azienda deve comprendere l'importanza e il valore dei dati, nonché degli ingenti danni economici legati a una perdita di informazione Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone:

- Il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare i danni;
- Potrà decidere di non informare gli interessati se riterrà che la violazione non comporti un rischio elevato per i loro diritti oppure se dimostrerà di avere già adottato misure di sicurezza; oppure, infine, nell'eventualità in cui informare gli interessati potrebbe comportare uno sforzo sproporzionato al rischio. In questo ultimo caso, dovrà provvedere con una comunicazione pubblica;
- L'Autorità Garante potrà comunque imporre al titolare del trattamento di informare gli interessati sulla base di una propria valutazione dei rischi correlati alla violazione commessa.

Molti esperti ritengono di essere davanti ad un cambiamento epocale in materia di protezione dei dati personali, in quanto il regolamento mira a raggiungere concretamente la tutela del diritto dell'individuo, al controllo sui propri dati personali; il tutto affidando a ogni singolo titolare le scelte per garantire detto diritto. Ebbene le principali novità introdotte dal Regolamento sono:

1) Principio di accountability o Responsabilizzazione/Rendicontazione;

2) Introduzione dei principi di privacy by design e privacy by default;

3) il Data Protection Officer (DPO);

4) Registro dei trattamenti;

5) valutazione di impatto (DPA);

6) Procedura di data breach;

7) Rilascio del consenso e la possibilità per i minori di prestare la propria

autorizzazione per i servizi (quali Facebook, Instagram ecc…);

8) Contenuto dell'informativa;

9) Nuovi diritti dell'interessato (portability, diritto all'oblio, diritto all'accesso, ecc…).

La protezione dei dati deve rappresentare una priorità nelle strategie di gestione del rischio anche degli studi professionali, stante la sensibilità delle informazioni trattate.

Si pensi, ad esempio, ai dati trattati dagli studi medici o dagli avvocati e ancor di più dai penalisti. Di conseguenza anche gli studi professionali dovranno adeguarsi al Regolamento e all'uopo dovranno adottare misure organizzative e tecniche volte a garantire un livello di sicurezza idoneo al rischio sia informatico che legale, legato al trattamento del dato del proprio cliente.

Le disposizioni della presente direttiva si applicano al trattamento di dati personali interamente o parzialmente automatizzato nonché al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi (D 95/46/CE). Il presente regolamento si applica anche al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi (GDPR)[5].

Il Codice si applica a chi è stabilito in Italia, anche se i dati sono detenuti all'estero. Viceversa chi è stabilito fuori dall'UE, esso si applica a chi impiega strumenti situati in Italia. Gli strumenti servono solo al transito dei dati nel territorio dell'UE e quando gli si applica il codice e per consentirne l'applicazione il titolare designa un rappresentante dedito alla sua realizzazione.

In definitiva il D.Lgs. n.101/18 è stato emanato al fine di armonizzare il Codice Privacy con tali innovazioni legislative, mettendo a punto quelle precisazioni che lo stesso GDPR demandava alla scelta discrezionale dei singoli Paesi membri.

2. Data Protection Officer (DPO) - Mansioni

Il DPO è una delle novità introdotte dal regolamento europeo per la protezione dei dati personali 679/2016 (Regolamento o GDPR). Il DPO, figura storicamente già

[5] Ambito di eccezione: trattamenti effettuati da persone fisiche per scopi personali o familiari.

presente in alcune legislazioni europee, 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. Questo soggetto è già conosciuto nel mondo anglosassone con il termine di *Chief Privacy Officer* (CPO); *Privacy Officer, Data Protection Officer o Data Security Officer*.

La sua responsabilità principale è quella 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.

Infatti esso supporta l'attività del Titolare del trattamento dati ovvero di supervisione dei profili di responsabilità giuridica derivanti dall'applicazione del principio di *accountability*[6].

Questa nuova professionalità, che il regolamento richiede sia individuata in funzione delle qualità professionali e della conoscenza specialistica della normativa e della prassi in materia di protezione dati, costituisce il fulcro del processo di attuazione del principio di "responsabilizzazione". Il diretto coinvolgimento del DPO in tutte le questioni che riguardano la protezione dei dati personali, sin dalla fase transitoria, è sicuramente garanzia di qualità del risultato del processo di adeguamento in atto. In questo ambito, sono da tenere in attenta considerazione i requisiti normativi relativamente a: posizione (riferisce direttamente al vertice), indipendenza (non riceve istruzioni per quanto riguarda l'esecuzione dei compiti) e autonomia (attribuzione di risorse umane e finanziarie adeguate). Particolare rilievo riveste il requisito dell'indipendenza del DPO (è riportato testualmente che il DPO deve "poter adempiere alle funzioni e ai compiti in maniera indipendente"), a prescindere che sia un dipendente o meno del Titolare del trattamento, ed il requisito dell'autonomia intesa nel senso che devono essergli attribuite le risorse necessarie per assolvere ai propri compiti.

I DPO non rispondono personalmente in caso di inosservanza del GDPR. Quest'ultimo chiarisce che spetta al titolare del trattamento o al responsabile del

[6] Nella versione in lingua inglese del GDPR (articolo 5, comma 2) si rinviene il principio di "accountability" come criterio guida del Regolamento per la protezione dei dati personali. In italiano è stato tradotto con il termine "responsabilizzazione" ma il concetto non è chiaramente interpretabile solo come "responsabilità". Sarebbe molto limitativo e non pienamente conforme all'approccio voluto invece dal legislatore.

trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del regolamento stesso
(articolo 24, paragrafo 1). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare del trattamento o sul responsabile del trattamento.

Per quanto riguarda la nomina di un DPO, l'articolo 37 non distingue fra titolari del trattamento e responsabili del trattamento in termini di sua applicabilità. A seconda di chi soddisfi i criteri relativi all'obbligatorietà della nomina, potrà essere il solo titolare del trattamento ovvero il solo responsabile del trattamento, oppure sia l'uno sia l'altro a dover nominare un DPO; questi ultimi saranno poi tenuti alla reciproca collaborazione. Vale la pena di evidenziare che anche qualora il titolare del trattamento sia obbligato a nominare un DPO, il suo eventuale responsabile del trattamento non è detto sia egualmente tenuto a procedere a tale nomina – che però può costituire una buona prassi. Il DPO nominato dal responsabile del trattamento vigila anche sulle attività svolte quando il responsabile operi in qualità di autonomo titolare del trattamento – per esempio, rispetto ai dati concernenti il personale, le risorse informatiche, la logistica. Per quel che concerne gli studi professionali ebbene si dovrà valutare rigorosamente se si è obbligati o meno alla nomina. Il GDPR all'art. 37 prevede i casi in cui la nomina è obbligatoria. Per gli studi professionali bisognerà seguire tali predisposizioni: a) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; b) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati, come quelli biometrici, sanitari, genetici o di dati personali relativi a condanne penali e reati[7].

Dopo questa breve premessa, adesso passeremo in rassegna i compiti ed i requisiti professionali che deve avere un DPO.

[7] Per **monitoraggio regolare** si intende: - in corso o che si verifica a intervalli specifici per un determinato periodo; - ricorrente o ripetuto in tempi fissi; - costante o periodico.
Per **monitoraggio sistematico**: - si svolge attraverso un sistema, una strategia, preorganizzato, organizzato o metodico; - si svolge nell'ambito di un piano generale per la raccolta dei dati (salute attraverso dispositivo indossabili; - utilizzo di telecamere a circuito chiuso; ecc..).
Per **trattamenti su larga scala**: - il numero degli interessati coinvolti; - il volume dei dati trattati; - la durata delle attività di trattamento o l'estensione geografica del trattamento.

Il DPO deve possedere, in particolare, una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati nonché la capacità di svolgere i compiti di cui all'articolo 39 e, cioè:

- informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che trattano i dati personali;
- sorvegliare l'osservanza della normativa comunitaria e nazionale nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento riguardanti anche "l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo";
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- cooperare con l'autorità Garante nazionale;
- fungere da punto di contatto per l'autorità Garante nazionale 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.

In relazione ai compiti va peraltro precisato che l'elenco di cui all'art. 39 costituisce una base minimale in quanto rappresenta quelli che il DPO deve svolgere "comunque", con ciò presupponendo la possibilità, per il Titolare o il Responsabile del trattamento, di aggiungerne altri.

Anche interessante risulta la precisazione, contenuta nel medesimo articolo, che il DPO, nello svolgimento dei propri compiti, non deve perdere mai di vista il "rischio da trattamento", tenendo conto dei seguenti parametri del trattamento stesso:

- natura;
- ambito di applicazione;
- contesto;
- finalità.

Dall'esame dei compiti emerge la necessità che il DPO, come già precisato in premessa, abbia adeguate competenze sia manageriali che in ambito giuridico, informatico nonché nei settori del *risk management* e dell'analisi processuale di cui, peraltro, la recente norma UNI 11697:2017 fornisce una descrizione

dettagliata.

Inoltre, nelle FAQ del sito dell'Autorità Garante nazionale è precisato che il DPO deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento. Deve poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il Titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare.

In pratica sono sicuramente più importanti competenze di base consolidate negli ambiti legale, informatico e gestionale ma non necessariamente particolarmente approfondite, piuttosto che essere esperti di una materia e non conoscere nulla delle altre, tanto più che il DPO potrà essere supportato da un team di specialisti, interni o esterni all'organizzazione.

Per il DPO non sono previste le certificazioni di cui all'art. 42 del GDPR anche se si stanno diffondendo alcune certificazioni "proprietarie", legate a specifici percorsi formativi, che costituiscono una presunzione "semplice" di idoneità professionale il cui valore è rimesso al "prudente apprezzamento" dei Titolari che, pertanto, non sono esonerati dal valutare in concreto i requisiti del DPO. Per l'efficace svolgimento delle proprie attività, sono riconosciuti specifiche prerogative e attribuiti determinati doveri. All'uopo il Gruppo "articolo 29" ha emanato le linee guida WP 243 rev. 01 (versione aggiornata del 5 aprile 2017).

Il 13 settembre 2018 il TAR per il Friuli Venezia Giulia, con la sentenza n°287/18, ha emesso una delle primissime decisioni in tema di nomina del Responsabile per la protezione dei dati personali (RPD o, nella variante anglofona, DPO, *Data Protection Officer*), prevista dal Regolamento Generale per la Protezione dei Dati (RGPD o, nella variante anglosassone e più comune, GDPR).

La sentenza ha origine dalla dichiarazione di inammissibilità di una domanda di partecipazione ad un avviso pubblico di un'Azienda sanitaria relativo all'affidamento dell'incarico di collaborazione professionale come DPO.

Il summenzionato avviso pubblico, infatti, dopo aver evidenziato l'impossibilità di individuare la figura del DPO tra i dipendenti della medesima amministrazione, disponeva la selezione per titoli ed eventuale colloquio, di un esperto sulla normativa e sulla prassi in materia di protezione dei dati al quale affidare l'incarico di collaborazione professionale per "l'impostazione e lo svolgimento nella fase di prima applicazione" dei compiti di DPO.

In base all'oggetto dell'avviso pubblico, il soggetto prescelto, oltre a dover svolgere i compiti tipici del DPO (previsti dall'art. 39 del GDPR), avrebbe dovuto svolgere le seguenti ulteriori funzioni: "l'aggiornamento giuridico e impostazione organizzativo-metodologica per la gestione aziendale della privacy, per la redazione del registro dei trattamenti, per lo svolgimento di valutazioni di impatto sulla protezione dei dati (DPIA)"; la ricognizione ed *assessment* aziendale in termini di sicurezza informatica e privacy, avendo riguardo, tra l'altro, alla conformità al GDPR, alle misure minime di sicurezza per la PA di cui alla Circolare AgID n. 2/2017, alle criticità emerse, alla contrattualistica con i fornitori, agli applicativi esistenti di cui si sarebbe dovuta svolgere una verifica di *compliance* rispetto al principio di privacy by design; la "partecipazione alle attività di formazione interna continua e specifica sulle tematiche della protezione dei dati".

In sostanza il soggetto individuato come DPO avrebbe dovuto eseguire una serie di compiti specifici ulteriori rispetto a quelli previsti dall'art. 39 del GDPR.

Ma il punto più rilevante dell'avviso pubblico riguarda proprio i requisiti di partecipazione alla selezione. In esso si richiedeva, infatti, "il possesso, in capo a ciascun candidato, del diploma di laurea in Informatica o Ingegneria Informatica, ovvero in Giurisprudenza o equipollenti, nonché la certificazione di "*Auditor/Lead Auditor"* per i Sistemi di Gestione per la Sicurezza delle Informazioni secondo la norma ISO/IEC/27001".

Il primo profilo, oggetto di analisi del ricorso, è quello relativo alla corretta interpretazione da attribuire al testo dell'avviso pubblico: non sarebbe possibile comprendere, sostiene il Tribunale, se la laurea in informatica, ingegneria informatica, giurisprudenza o equipollenti fosse o meno alternativa rispetto alla certificazione di auditor o *lead auditor* in base alla norma ISO/IEC/27001. Il

dubbio parrebbe doversi sciogliere nel senso della mancanza di una alternativa e risolversi, invece, a favore della interpretazione secondo la quale la certificazione auditor o *lead auditor* ISO27001 rappresentasse un requisito ulteriore rispetto ai titoli di laurea summenzionati (considerata la presenza della congiunzione "nonché"). Il secondo e, sembrerebbe più rilevante profilo affrontato nel ricorso era incentrato sul punto in cui l'avviso pubblico prevedeva (quale requisito ulteriore rispetto al possesso del diploma di laurea in Informatica o Ingegneria Informatica, ovvero in Giurisprudenza o equipollenti) la necessità che i candidati fossero dotati della "certificazione Auditor/Lead Auditor per i Sistemi di Gestione per la Sicurezza delle Informazioni secondo la norma ISO/IEC/27001". Il ricorrente, infatti, nella sua domanda di risposta all'avviso pubblico precisava di essere in possesso della laurea in giurisprudenza ma di non possedere, invece, "la certificazione Auditor/Lead Auditor per i Sistemi di Gestione per la Sicurezza delle Informazioni".

Tra i motivi portati dal ricorrente all'attenzione del Tribunale Amministrativo Regionale vi è, innanzitutto, il fatto che la previsione della richiesta, tra i requisiti, qualifica di Auditor o Lead Auditor ISO/IEC/27001 si porrebbe in antitesi logica rispetto all'apertura alla candidatura dei titolari di laurea in giurisprudenza. Oltretutto, si sostiene, le competenze richieste dall'avviso pubblico sarebbero maggiormente compatibili con quelle tipiche dei laureati in giurisprudenza piuttosto che con quelle dei laureati in informatica o ingegneria informatica.

Il TAR ha accolto il ricorso.

Nell'accogliere il ricorso il TAR motiva la propria decisione sulla scorta delle seguenti considerazioni. In primo luogo la certificazione 27001 "non costituisce un titolo abilitante" per le funzioni di DPO posto che la norma ISO27001 trova prevalente applicazione nell'ambito dell'attività d'impresa e, comunque, la minuziosa conoscenza e l'applicazione della disciplina di settore restano, indipendentemente dal possesso o meno della certificazione in parola, il nucleo essenziale ed irriducibile della figura professionale ricercata dall'Azienda, il cui profilo, per le considerazioni anzidette, non può che qualificarsi come eminentemente giuridico. La certificazione in oggetto, inoltre, secondo il TAR, non può costituire requisito di ammissione (né equipollente al titolo di

laurea richiesto) in quanto non coglie la specifica funzione di garanzia insita nell'incarico conferito, il cui precipuo oggetto non è costituito dalla predisposizione dei meccanismi volti ad incrementare i livelli di efficienza e di sicurezza nella gestione delle informazioni ma attiene semmai alla tutela del diritto fondamentale dell'individuo alla protezione dei dati personali. E tale conclusione sarebbe confermata sulla scorta dell'analisi dei programmi dei corsi finalizzati all'acquisizione della certificazione ISO/IEC/27001 prodotti dal ricorrente che si caratterizzano per una durata contenuta e per la "netta prevalenza delle tematiche attinenti all'organizzazione aziendale (e ciò a discapito dei profili giuridici) e dall'assenza di contenuti riferibili all'attività e alla struttura delle pubbliche amministrazioni. Oltretutto, si soggiunge, i dirigenti incaricati dalle Aziende resistenti, nelle more del giudizio, dei compiti di DPO non erano, comunque, in possesso della certificazione ISO/IEC/27001, e ciò confermerebbe ulteriormente la sua irrilevanza ai fini dello svolgimento dell'incarico di DPO.

In definitiva, la sentenza in questione giunge ad una conclusione condivisibile sia pur conservando, nel percorso argomentativo, alcuni aspetti oscuri e che lasciano spazio a perplessità, considerando anche la novità legislativa con l'introduzione del DPO.

I presupposti per la corretta individuazione della figura del DPO – sia da parte di soggetti pubblici che privati – sono racchiusi nella norma del quinto comma dell'art. 37 del GDPR, in base al quale 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*". Di primaria importanza nell'interpretazione dei criteri di scelta è anche il considerando 97 del GDPR in base al quale il DPO dovrebbe essere "*una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno*" del GDPR e, infine, "*il livello necessario di conoscenza specialistica dovrebbe essere determinato in particolare in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento*". Ad ulteriore specificazione delle modalità di individuazione del DPO assumono rilevanza

fondamentale le linee guida sui responsabili della protezione dei dati adottate dall'**Art. 29WP**[8]. Le linee guida, anzitutto, prevedono la possibilità (in linea rispetto a quanto previsto dal considerando 97 del GDPR) di distinguere il livello di conoscenze specialistiche richiesto al DPO a seconda, caso per caso, della complessità del trattamento o del volume di dati sensibili oggetto del trattamento. Inoltre, si evidenzia come le qualità professionali da prendere in considerazione per la nomina del DPO non siano affatto specificate dall'art. 37 del GDPR. Pur non essendo individuate chiaramente le qualità professionali richieste, appare chiaro che il DPO debba avere conoscenze sulla normativa e sulle prassi nazionali ed europee in materia di protezione dei dati, ivi compreso il GDPR. Inoltre, il DPO dovrebbe conoscere lo specifico settore (in cui eserciti la sua professionalità), le operazioni di trattamento ivi svolte e le esigenze di sicurezza manifestategli dal titolare. Inoltre, il DPO operante nella PA, dovrebbe avere una familiarità con le norme e le procedure amministrative di riferimento. Sempre le linee guida dell'Art.29WP, ad ulteriore specificazione delle competenze specialistiche che dovrebbero caratterizzare il DPO, indicano: familiarità con tecnologie informatiche e misure di sicurezza dei dati; capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione del titolare o del responsabile. Da questo punto di vista è chiaro che la motivazione della sentenza del TAR, nel passaggio in cui statuisce che il profilo del DPO "non può che qualificarsi come eminentemente giuridico" non può intendersi nel senso di limitarne l'esercizio esclusivamente ai giuristi ma, invero, nel senso che a prescindere dal titolo di studio, in ogni caso, il DPO non possa non avere – ed essere in grado di dimostrarle –competenze nell'ambito giuridico così come delineato dall'Art. 29WP (ossia normativa e prassi nazionali ed europee in materia di protezione dei dati, compresa un'approfondita conoscenza del GDPR). La prima considerazione che porta a ritenere corretta la decisione in esame nel punto in cui esclude che possa prevedersi quale condizione essenziale allo svolgimento dell'attività di DPO la qualifica di auditor o *lead auditor* ISO/IEC/27001 è quella secondo la quale le competenze specialistiche richieste al DPO (in base al GDPR e all'interpretazione della norma data dall'Art.29WP) variano a seconda

[8] Attualmente il Comitato europeo per la protezione dei dati personali.

dell'ambito in cui si troverà ad operare. La questione del "bollino" oltretutto era già stata risolta dal Garante privacy nel senso che – come previsto nelle FAQ del Garante in tema di responsabile della protezione dei dati personali – gli schemi proprietari di certificazione volontaria delle competenze professionali (che non rientrano tra quelle disciplinate dall'art. 42 del GDPR) 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 DPO né, allo stato, sono idonee a sostituire il giudizio rimesso alle PP.AA. nella valutazione dei requisiti necessari al DPO per svolgere i compiti previsti dall'art. 39 del GDPR".

Anche per tale ragione la PA non può sostituire un giudizio effettivo sulle capacità del candidato (basato sulla verifica delle effettive competenze specialistiche piuttosto e non sul "massimo ribasso" offerto) al possesso, da parte del medesimo, di bollini o abilitazioni non previsti dal GDPR.

Per questo motivo, perciò, potrà anche tenersi in considerazione – nell'analisi comparativa delle esperienze professionali e del bagaglio di esperienze del singolo candidato a ricoprire il ruolo di DPO – delle eventuali abilitazioni, certificazioni, attestati di partecipazione a corsi etc., ma questi non potranno rappresentare una barriera illogica e condizionante la partecipazione al procedimento di selezione.

Dopo l'analisi di questo primissimo provvedimento in materia di DPO passiamo alle conclusioni di questo articolo non sottovalutando però un aspetto fondamentale che sembra sfuggire a qualcuno, in relazione alla professionalità che il DPO deve possedere. A seguito della nomina ricevuta, molti credono che sia sufficiente integrare le proprie competenze attraverso seminari, corsi, letture, ecc., ricercando impossibili "*upgrade*"specialistici.

Sicuramente tutto ciò è molto utile in quanto serve per sviluppare praticità nel settore, acquisire padronanza con i termini appropriati ecc., ma per poter effettivamente svolgere i complessi compiti devoluti a questa figura, occorre la presenza di varie e approfondite conoscenze specialistiche riferite non solo al settore giuridico ma anche organizzativo, manageriale e tecnologico. Insomma si tratta di una vera e propria professione che richiede un esperienza consolidata che solo un *Team* di professionisti è in grado di realizzare; con la consapevolezza

anche di doversi integrare all'interno dell'ambiente organizzativo al solo fine di adempiere correttamente alle finalità preposte.

LA RESPONSABILITÀ DEL RESPONSABILE DELLA PROTEZIONE DATI (DATA PROTECTION OFFICER – DPO)

di Gianluca Bozzelli

SOMMARIO: 1. Premessa; 2. La responsabilità contrattuale del DPO esterno; 3. Le responsabilità del DPO interno: contrattuale, disciplinare ed amministrativa; 4. La responsabilità penale.

1. Premessa

Nell'esaminare brevemente le responsabilità del DPO, emerge la necessità che si verifichi un danno, nell'esercizio delle attività di trattamento dei dati personali, di cui sarà ritenuto responsabile il titolare o il responsabile del trattamento dati, come previsto dall'art. 82 GDPR.

È da tale premessa che si deve muovere, nell'esaminare la responsabilità del D.P.O., in quanto questi è nominato e designato da titolare e responsabile, ai sensi dell'art. 37 comma 1 del GDPR.

Nell'esecuzione dei compiti elencati dal GDPR (nonché degli altri che potrebbero essere assegnati in via contrattuale, per mezzo del relativo incarico di nomina, poiché si tratta di un'elencazione chiaramente non tassativa, come conferma la formulazione normativa, nel punto in cui prescrive che tale soggetto sia "incaricato almeno" dei compiti menzionati nei punti successivi) il DPO non è direttamente responsabile, civilmente nei confronti di terzi. Allo stesso non possono essere neppure imputate eventuali sanzioni amministrative inflitte al titolare. Ciò non esclude, eventualmente, l'assunzione di responsabilità in sede contrattuale, per mezzo di manleve ed esoneri di responsabilità a favore del titolare o del responsabile. Sotto tale profilo, infatti, si consideri che il DPO è (art. 37 comma 5) "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 comma successivo (6) chiarisce che oltre alle ipotesi in cui il DPO sia un dipendente del titolate o del responsabile, egli ben può assolvere i suoi compiti in base ad un contratto di servizi. Si tratta, con tutta evidenza, nel secondo caso, di un'attività di consulenza, con le responsabilità, prive di rilevanza esterna, di

natura civilistica tra consulente professionale e cliente (rapporto nel quale il titolare/responsabile è evidentemente il cliente del professionista).
Si ritiene che la responsabilità del DPO non abbia rilevanza esterna (direttamente nei confronti dell'interessato), in quanto l'art. 82 (a differenza dell'art. 15 Codice Privacy abrogato) individua esplicitamente come responsabili del danno, il titolare nel trattamento oi il suo responsabile. Con il GDPR cambia innanzitutto la prospettiva, rispetto alla precedente tutela risarcitoria citata, che estendeva la responsabilità derivante dal trattamento dati personali a "chiunque" avesse cagionato il danno, invocando l'art. 2050 cod. civ. (responsabilità per l'esercizio di attività pericolose).
La logica sottesa alla precedente normativa era quella di garantire l'inversione dell'onere probatorio in capo a chi gestisce i dati personali, con possibilità di escluderla solo laddove costui provasse che l'evento dannoso non gli è imputabile, avendo dato prova di aver adottato tutte le misure idonee ad evitare il danno (in tal senso lo stesso art. 23 della DIR. 46/95/CE che aveva portato alla normativa italiana del '96).
L'attuale art. 82 GDPR e il Considerando 146, al pari della Dir. del 95, stabiliscono che il titolare/responsabile possa essere esonerato dalla responsabilità conseguente al danno da illecito trattamento "se dimostra che l'evento dannoso non gli è in alcun modo imputabile" (onere della prova a carico del gestore dei dati e rigorosità della medesima prova). Pertanto, in attesa di ulteriori chiarimenti in attesa della giurisprudenza nazionale, sembra che i criteri cui è fondata l'interpretazione pretoria nella vigenza del Codice privacy possa essere, per dir così, recuperata anche alla luce del GDPR, il modello di responsabilità pare, pertanto, essere quello dell'art. 2050 cod. civ.
Chiarito, pertanto, che la responsabilità del DPO è sostanzialmente interna al rapporto contrattuale tra consulente/funzionario e titolare/responsabile, potrebbe al più rinvenirsi una responsabilità concorrente con quella personale e diretta del DPO, laddove il danneggiato configurasse un'attività illecita anche ultronea o esorbitante le attività tipicamente proprie del trattamento dati (in misura del tutto astratta potrebbe immaginarsi il caso della diffusione volontaria ed in ambiti del tutto estranei al trattamento, derivanti da una conoscenza personale del DPO).

Si pensi anche al caso di aggravamento del danno, come recentemente affermato dalla Suprema Corte, che abbia dato luogo a condotte pregiudizievoli poste in essere da soggetti diversi dagli autori della divulgazione, non può, per ciò solo, escludersi l'esistenza – tra tale comportamento ed il danno lamentato – del nesso causale, dovendo la sua ricorrenza essere comunque affermata qualora risulti che le condotte dei terzi non sarebbero state possibili se non fossero stati resi noti i dati personali dei danneggiati»[9].

2. La responsabilità contrattuale del DPO esterno

Fatta la doverosa minima chiarificazione sui soggetti del danno, la responsabilità del DPO è pertanto connessa all'incarico di designazione e alla qualità rivestita dal designato.

Ai sensi dell'art. 38 comma 6, infatti, questi può essere un dipendente del titolare o del responsabile del trattamento, oppure assolvere i propri compiti in base a un contratto di servizi.

Vengono in rilievo, pertanto, le due ipotesi, che distinguono il tipo di responsabilità.

Nel primo caso, si tratterà di una tipica responsabilità professionale, derivante dalla violazione degli obblighi di diligenza specifica (art. 1176 comma 2 cod. civ.) e da inadempimento (art. 1218 cod. civ.) che, qualora la prestazione richieda la soluzione di problemi tecnici di speciale difficoltà esime da responsabilità se non in caso di colpa grave o dolo (art. 2236 cod. civ.). Nel caso in cui si tratti di dipendente (con poteri rafforzati e sotto posizione gerarchica ai soli vertici apicali (quadro o funzionario), si tratterà di una responsabilità nell'ambito del rapporto di lavoro (quindi ancora contrattuale), ma anche disciplinare e, in caso di ente pubblico, o equiparato, anche amministrativa e contabile.

Più agevole è chiaramente la disamina delle ipotesi di responsabilità contrattuale del professionista in relazione ai compiti di cui all'art. 39.

Inutile disquisire oltre, in questa sede, della responsabilità del professionista derivante da un'errata consulenza, poiché la produzione giurisprudenziale ed arbitrale è talmente ampia da rendere sufficiente in questa sede il solo riferimento.

[9] Cass. Civ. del 19.7.2016, n. 14694.

Poiché la prestazione del DPO implica la soluzione di problemi tecnici di speciale difficoltà, il prestatore d'opera non risponde dei danni, se non in caso di dolo o di colpa grave.

Il DPO, infatti, per essere nominato ha dichiarato di (ed è stato scelto per) essere particolarmente esperto e di avere una conoscenza specifica di normativa e prassi. Il DPO viene infatti designato "in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati" (art. 37, comma 5 GDPR). Sotto il profilo della specializzazione, il Garante privacy italiano [10] ha affermato che non sono previsti albi o altri organismi professionali per tale figura, né specifici percorsi formativi o certificazioni.

Deve ritenersi che l'esperienza nel settore sia sufficiente per rivestire il ruolo in esame, purché in qualche modo attestabile. Sul punto, il Garante ha affermato che eventuali certificati, rilasciati al termine di un percorso formativo, sebbene costituiscano "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 possono sostituire la valutazione fatta dal titolare o dal responsabile del trattamento sui requisiti del DPO che si intende nominare.

La *ratio* di tale dichiarazione può rinvenirsi, da un lato nella complessità del tipo di formazione necessaria, dall'altro con la necessità di escludere il propagarsi (effettivamente poi non impedito) di corsi di formazione e specializzazione da parte di enti che pretendano di avere potere certificativo.

Facendosi riferimento ad una conoscenza specialistica della normativa, il GDPR indica (non espressamente ma implicitamente) come consulente/funzionario RPD un esperto della normativa e della prassi: quindi necessariamente un giurista, collaborato o meno, da un tecnico specializzato nelle procedure. La nozione di "prassi in materia di protezione dei dati", infatti, sembra far riferimento ad elementi tecnici, quali la conoscenza di sistemi informatici e di misure di sicurezza. La particolare elasticità della previsione, consente di individuare esperti, in funzione della natura dei dati e delle tipologie dei trattamenti da

[10] Garante per la protezione dei dati personali, Provv. del 28.7.2017.

eseguirsi (si pensi ai casi di trasferimento all'estero o ai dati sanitari).

Poiché il DPO può essere designato tanto dal titolare quanto dal responsabile (art. 37 comma 1), è opportuno distinguere la responsabilità del consulente/funzionario anche in relazione alla provenienza della designazione. Nulla quaestio se la nomina è stata fatta direttamente dal titolare, qualora sia fatta dal responsabile (che ai sensi dell'art. 28 comma 3 lett. a tratta i dati personali "soltanto su istruzione documentata del titolare del trattamento"), potrebbe rinvenirsi una *deminutio* del suo livello di responsabilità, in corrispondenza dei limiti a sua volta applicabili al responsabile del trattamento (alcuni argomentando ex art. 28 GDPR, ritengono che il responsabile del trattamento possa essere solo esterno).

Il DPO esterno, ai sensi dell'art. 37 comma 6, viene designato sulla base di un contratto di servizi. Come ha affermato il Garante Privacy (pubblicando sul proprio sito internet, un modello di atto di designazione) è necessario che nella nomina "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". La scelta del DPO dovrà pertanto risultare esplicitata per consentire agli interessati ed alle autorità "la verifica del rispetto dei requisiti previsti dall'art. 37, comma 5 del GDPR, 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 e di buona amministrazione, costituisce anche elemento di valutazione del rispetto del principio di «responsabilizzazione"[11].

Sebbene tale indicazione del Garante faccia esplicito riferimento all'ambito pubblico, si ritiene che ben possa essere utilizzato come guida per la designazione anche in ambito privato, rispondendo i criteri indicati ai principi generali del GDPR (responsabilizzazione *in primis*) che devono essere rispettati da tutti gli enti titolare del trattamento, pubblici o privati che siano.

[11] Faq sul Responsabile della Protezione dei dati – RPD – in ambito pubblico del 15.12.2017, cit.

Si è detto che i compiti del RPD sono indicati in maniera non tassativa all'art. 39, per cui la casistica delle responsabilità civili del DPO esterno nei confronti del titolare non può essere predeterminata, dovendosi valutare caso per caso, in considerazione dello specifico compito o funzione che si assumono violati o non eseguiti, al punto da determinare un danno ingiusto agli interessati o l'applicazione di una sanzione amministrativa da parte di un'Autorità.

Nel caso di DPO esterno, si immagina, pertanto, che i professionisti candidati alla designazione a DPO siano forniti di assicurazione per la responsabilità professionale (laddove giuristi, estesa alla fase della consulenza stragiudiziale ed agli incarichi non giudiziali: cosa non comune), in modo da poter adeguatamente fronteggiare le prevedibili richieste di manleva e di esonero di responsabilità da parte dei designatori. È agevole prevedere che tali clausole contrattuali saranno inserite negli atti di nomina.

3. La responsabilità del DPO interno: contrattuale, disciplinare ed amministrativa

Più particolare e specifica appare, invece, la responsabilità del DPO interno.

Il comma 6 dell'art. 37 GDPR stabilisce che "Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento". Il DPO può essere anche un soggetto interno alla struttura del titolare del trattamento o del responsabile del trattamento.

La specificazione dei criteri utilizzati nella valutazione compiuta dall'ente nella scelta di tale figura, oltre a essere indice di trasparenza e di buona amministrazione, costituisce anche elemento di valutazione del rispetto del principio di *accountability*.

Nel caso degli enti di diritto pubblico, è richiesto che il DPO abbia una conoscenza approfondita non solo della normativa in materia di protezione di dati personali, ma altresì "delle norme e procedure amministrative che caratterizzano lo specifico settore, in quanto la liceità del trattamento dei dati personali in questo ambito dipende dalla corretta applicazione delle regole di volta in volta previste dalla disciplina speciale"[12]. Analogamente sarà necessario selezionare un DPO

[12] Garante per la protezione dei dati personali, Provv. 28.7.2017, nonché WP29, 12: "Nel caso di un'autorità pubblica o di un organismo pubblico, il RPD dovrebbe possedere anche una

che conosca lo specifico settore dei dati trattati dal titolare del trattamento nell'ambito della propria attività (ad esempio sanitario o merceologico in cui opera il titolare del trattamento).

Vengono in evidenza, a riguardo, le prescrizioni dell'art. 38 GDPR, per individuare le caratteristiche (e le conseguenti responsabilità) del DPO interno. Interpretando le disposizioni normative (comma 1), il responsabile della protezione dati dovrà essere tempestivamente e adeguatamente coinvolto in tutte le questioni dal titolare/responsabile, sostenuto nell'esecuzione dei compiti, mediante fornitura delle risorse necessarie e per mantenere la propria conoscenza specialistica: con evidenti obblighi di formazione professionale (comma 2). Che si tratti di un funzionario di alto grado (almeno quadro o diligente) è specificato espressamente (comma 3), poiché gli viene riconosciuta piena autonomia gestionale nell'esecuzione delle attività, immunità da rimozioni o penalizzazioni per l'adempimento dei propri compiti ed il diritto a riferire direttamente ai vertici apicali del titolare/responsabile. Tale qualifica è espressamente prevista dal Garante Privacy[13], il quale suggerisce che la figura di DPO interno sia ricoperta da "un dirigente ovvero da 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 dirigente in generale, in ambito pubblico o privato che sia, in quanto lavoratore subordinato, ha nei confronti del proprio datore di lavoro una responsabilità contrattuale (responsabilità interna) che gli deriva dalla legge, dal contratto collettivo e dal contratto individuale di lavoro. Egli deve eseguire la prestazione lavorativa con correttezza e buona fede ed è soggetto agli obblighi di fedeltà e diligenza, come disposto dagli artt. 2104 e 2105 cod. civ. Nell'ambito di un rapporto di lavoro di natura privatistica, nell'esecuzione delle proprie funzioni, però, il dirigente svolge un'attività che non ha rilevanza solamente interna, cioè solo nei confronti del proprio datore di lavoro. Spesso, infatti, soprattutto se munito di procura, impegna la società nei confronti di terzi (soci, clienti, fornitori) e, comunque, per il suo ruolo può condizionare il buon funzionamento aziendale, incidendo sulla posizione di soggetti esterni. Un eventuale fatto illecito commesso

conoscenza approfondita delle norme e procedure amministrative applicabili".

[13] Nuove Faq del 15.12.2017, cit.

nei confronti di terzi dà origine alla responsabilità extra-contrattuale (responsabilità esterna), responsabilità civile ma anche penale, se il fatto illecito costituisce reato. Le norme dei CCNL generalmente disciplinano espressamente la responsabilità civile e penale per fatti illeciti compiuti dal dirigente verso terzi nell'esercizio della sua prestazione lavorativa, limitandola alle ipotesi di dolo o colpa grave.

Perché sia rinvenibile responsabilità personale del dirigente deve essergli stato attribuito l'effettivo potere e la necessaria autonomia decisionale: la delega deve risultare da un atto formale, emanato da chi ne abbia il potere. La responsabilità civile e le conseguenze risarcitorie a favore di terzi danneggiati per fatti commessi dal dirigente nell'esercizio delle sue funzioni, pertanto, rimangono a carico del datore di lavoro.

Il dirigente è oggi titolare di una serie di situazioni passive di dimensioni variabili, la cui inottemperanza può dar luogo non solo ad inadempimento per l'esecuzione della prestazione in modo derogatorio agli obblighi (di diligenza e di fedeltà e di non concorrenza) ma anche a qualificazioni che sfuggono dalla dicotomia adempimento/inadempimento degli obblighi contrattuali.

Qualsiasi generalizzazione in ordine alla posizione del dirigente, sia ai fini dell'imputazione di reati sia ai fini della responsabilità contrattuale per inadempimento, può condurre facilmente ad equivocare; bisogna tener conto della specifica "competenza" o meglio delle mansioni affidate a ciascuno nello specifico settore produttivo. Il contenuto della prestazione lavorativa appare però caratterizzata dal ricorrere costante ed in modo identico in rapporto a tutti i livelli funzionali di una connotazione costituita dalla responsabilità del dirigente assunta per il raggiungimento del risultato gestionale afferente alla porzione di attività affidata. In tal senso, pertanto, anche qualora fosse incaricato della protezione dei dati personali, verrebbe in rilievo il risultato aziendale prefissato dai vertici apicali dell'ente che, sebbene non foriero di danno a terzi, potrebbe generare una responsabilità del DPO interno per mancato raggiungimento del risultato.

Quanto alle ulteriori funzioni che possono essere affidate, in linea di principio, è ragionevole pensare che negli enti pubblici di grandi dimensioni, con trattamenti di dati personali di particolare complessità e sensibilità, non vengano assegnate al

DPO interni ulteriori responsabilità (art. 38 comma 6): il DPO può svolgere altri compiti e funzioni ma il titolare/responsabile si assicura che tali compiti e funzioni non diano adito ad un conflitto di interessi e che lo stesso possa mantenere la propria formazione professionale (comma 2). Si pensi, ad esempio, alle amministrazioni centrali, alle agenzie, agli istituti previdenziali, nonché alle regioni e alle aziende sanitarie. In tale quadro, ad esempio, avuto riguardo, caso per caso, alla specifica struttura organizzativa, alla dimensione e alle attività del singolo titolare o responsabile, l'attribuzione delle funzioni di DPO al responsabile per la prevenzione della corruzione e per la trasparenza, considerata la molteplicità degli adempimenti che incombono su tale figura, potrebbe rischiare di creare un cumulo di impegni tali da incidere negativamente sullo svolgimento dei compiti attribuiti al DPO.

In ambito pubblicistico, il Testo Unico del pubblico impiego (D.Lgs. n.165/2011) attribuisce al dirigente pubblico poteri di manager, dai quali deriva una responsabilità di risultato legata al sistema di valutazione della performance, cosi come previsto dal Titolo II del D.Lgs. n.150/2009.

Pertanto, la responsabilità dirigenziale (definita dall'art. 21, comma 1) si allontana dai tradizionali tipi di responsabilità, che tendono a sanzionare un singolo comportamento riconosciuto come illegittimo, compiuto con dolo o colpa, ma intende sanzionare una condotta complessiva ritenuta non soddisfacente per il raggiungimento di obiettivi predefiniti e quindi soddisfare dei bisogni qualitativamente e quantitativamente ritenuti socialmente rilevanti. Pertanto, la peculiarità della responsabilità dirigenziale è non tanto quella di prevedere uno strumento punitivo o sanzionatorio, quanto piuttosto di fornire un meccanismo correttivo dell'organizzazione pubblica (art. 97 Cost.).

Degna di rilievo (e compatibile con il disposto dell'art. 37 comma 7 GDPR, che prevede la pubblicazione dei dati di contatto dei DPO e la comunicazione all'Autorità di controllo) è la pubblicizzazione degli incarichi dirigenziali attraverso la pubblicazione su un'apposita banca dati. Tale condotta realizza un'effettiva trasparenza, che consente di far emergere (e verificare) la professionalità di ogni singolo dirigente.

I dirigenti e tutti i funzionari pubblici sono imputabili per responsabilità civile,

penale amministrativo-contabile e disciplinare. Accanto alle forme tipiche, il TUPI ha riconosciuto per i dirigenti l'imputabilità della responsabilità dirigenziale, come aggiuntiva responsabilità individuale, imputabile solo ai soggetti titolari di funzioni dirigenziali e riferibile al complesso di attività di gestione e di organizzazione. Tale responsabilità specifica - elaborata proprio per rispondere ad una esigenza di controllo nei confronti dei dirigenti, che nell'ambito della distinzione delle competenze, divengono titolari di un ampio e autonomo potere di gestione – ben potrebbe essere invocata nel caso della gestione del trattamento dei dati personali, proprio in quanto settore di specifica competenza ed autonomia attribuita ad DPO interno. Poiché essa trova la sua definizione nel momento in cui al dirigente viene affidato un incarico dirigenziale, ovvero quando eserciterà la funzione manageriale in senso proprio, in quel caso, il DPO interno sarà imputabile per responsabilità dirigenziale. Il comma 4 dell'art. 55 *sexies* stabilisce che "la responsabilità civile eventualmente configurabile a carico del dirigente in relazione a profili di illiceità nelle determinazioni concernenti lo svolgimento del procedimento disciplinare è limitata, in conformità ai principi generali, ai casi di dolo o colpa grave".

La *ratio* sembra ravvisarsi nella circostanza per cui la responsabilità disciplinare è una responsabilità soggettiva con fondamento civilistico in quanto si basa sul presupposto che un dato comportamento sia imputabile all'attore a titolo di dolo o colpa.

Per quanto riguarda l'imputabilità, l'art. 21 comma 1 TUPI stabilisce due fattispecie principali: "mancato raggiungimento degli obiettivi" e "inosservanza delle direttive imputabile al dirigente". Entrambe le fattispecie di responsabilità producono i propri effetti nell'ambito del rapporto tra organo di indirizzo politico dell'ente pubblico ed organo di gestione amministrativa, nell'ambito della distinzione delle competenze. Può comportare il mancato rinnovo dell'incarico, la revoca dell'incarico e, nei casi più gravi, il recesso del rapporto di lavoro. La prima ipotesi rientra in un più ampio processo di cambiamento che ha caratterizzato la pubblica amministrazione a partire dalla legge n.142/90: l'amministrazione non ha più il solo obbligo di rispettare le norme e quindi il principio di legalità, ma anche soddisfare i bisogni e quindi raggiungere, nel modo

più efficiente possibile, i risultati predefiniti, rispondendo ai canoni di efficienza ed efficacia. La seconda ipotesi fa riferimento all'inosservanza delle direttive, quale possibilità che il dirigente non rispetti l'indirizzo proposto dall'organo politico, o meglio, si discosti dagli obiettivi e dalle direttive impartitegli: tale ipotesi trova la sua *ratio* nel rapporto di funzionalità che lega il dirigente amministrativo all'organo politico. Il dirigente, pur essendo titolare di ampi poteri pubblici di gestione, deve comunque rispettare le direttive affidategli.

Sotto il profilo disciplinare, la responsabilità trova la sua fonte, da un lato, nell'art. 28 Cost. che si preoccupa di sanzionare la violazione dei diritti perpetrata da atti delle amministrazioni affermando le conseguenti responsabilità dei funzionari e dei dipendenti, e dall'altro lato nell'art. 97 Cost. che tratta di responsabilità statuendo che "nell'ordinamento degli uffici sono determinate le sfere di competenza, le attribuzioni e le responsabilità proprie dei funzionari".

Il nuovo assetto della responsabilità disciplinare è significativo in quanto non riguarda più soltanto i "cattivi comportamenti" dei dipendenti pubblici, ma tutte le ipotesi di "cattiva amministrazione" che si riversano in disfunzioni dell'agire amministrativo. Inoltre, viene in evidenza l'art. 55 *sexies* TUPI rubricato "Responsabilità disciplinare per condotte pregiudizievoli per l'amministrazione e limitazione della responsabilità per l'esercizio dell'azione disciplinare".

Il primo comma del suddetto art., modificato dal d.lgs. n. 75/2017 in materia di riorganizzazione delle pubbliche amministrazioni, prevede che "La violazione di obblighi concernenti la prestazione lavorativa, che abbia determinato la condanna dell'amministrazione al risarcimento del danno, comporta comunque, nei confronti del dipendente responsabile, l'applicazione della sospensione dal servizio con privazione della retribuzione da un minimo di tre giorni fino ad un massimo di tre mesi, in proporzione all'entità del risarcimento, salvo che ricorrano i presupposti per l'applicazione di una più grave sanzione disciplinare".

Degno di rilievo è, inoltre, il terzo comma dell'art. 55 *sexies* TUPI, che ha riguardo, invece, ai casi di "mancato esercizio o decadenza dell'azione disciplinare dovuti all'omissione o al ritardo, senza giustificato motivo degli atti del procedimento disciplinare, inclusa la manifestazione di cui all'art. 55 *bis* comma 4 […] comporta, per i soggetti responsabili, l'applicazione della

sospensione dal servizio fino ad un massimo di tre mesi salva la maggiore sanzione del licenziamento […].

Tale condotta, per il personale con qualifica dirigenziale o titolare di funzioni o incarichi dirigenziali, è valutata anche ai fini della responsabilità di cui all'art. 21 del presente decreto. Ogni amministrazione individua preventivamente il titolare dell'azione disciplinare per le infrazioni di cui al presente comma commesse da soggetti responsabili dell'ufficio di cui all'art. 55 *bis*, comma 4."

La responsabilità dirigenziale, che come risulta dalla normativa non è meramente facoltativa ma obbligatoria. La teoria dell'obbligatorietà dell'azione disciplinare è altresì desunta dall'art. 55 *bis*, comma 7, del TUPI che prevede l'obbligo del dipendente o dirigente che è a conoscenza per ragioni di ufficio o di servizio di informazioni rilevanti per un procedimento disciplinare in corso, di prestare collaborazione all'autorità disciplinare, salvo la ricorrenza di un giustificato motivo.

Rispetto alla necessità che non si creino situazioni di conflitto di interessi (art. 38 comma 6 GDPR), occorre inoltre valutare se le eventuali ulteriori (o precedenti) mansioni assegnate al DPO interno non comportino la definizione di finalità e modalità del trattamento dei dati. Ciò implica che, in ambito pubblico, oltre ai ruoli manageriali di vertice, possono sussistere situazioni di conflitto di interesse rispetto a figure apicali investite di capacità decisionali in ordine alle finalità e ai mezzi del trattamento di dati personali posto in essere dall'ente, ivi compreso, ad esempio, il responsabile dei sistemi informativi (chiamato ad individuare le misure di sicurezza necessarie), ovvero quello dell'Ufficio di statistica (deputato a definire le caratteristiche e le metodologie del trattamento dei dati personali utilizzati a fini statistici).

Infine, l'art. 38, comma 5, prevede l'obbligo di segretezza e riservatezza in merito all'adempimento dei propri compiti: specificazione che in conformità con il diritto italiano, potrebbe configurare una responsabilità del DPO per violazione di questi specifici obblighi in danno del titolare o del responsabile del trattamento dei dati.

Meritevole di attenzione è poi il riferimento al "coinvolgimento" nello stesso trattamento. Con tale espressione, il GDPR intende riferirsi a qualsivoglia forma di partecipazione (sia attiva sia passiva e tenuto conto degli obblighi in capo a

ciascuna parte) nel trattamento causativo del danno. Tenuto, quindi, conto della previsione di cui al comma 3 dell'art. 82 (già esaminata), diventa imperativo definire in modo dettagliato, nelle policy privacy, le "istruzioni" che competono al titolare del trattamento e le previsioni contrattuali che disciplinato i doveri (obblighi) contrattuali del responsabile del trattamento. Ai sensi del comma 5 dell'art, 82 "Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2." La norma disciplina, con tutta evidenza (e coerentemente con quanto già sopra affermato), le conseguenze patrimoniali del danno nei rapporti interni: non vi è, pertanto, responsabilità solidale, ma responsabilità pro-quota.

Un aspetto concreto è quello dei "criteri di calcolo" del grado e della misura della responsabilità tra i vari soggetti responsabili. Una linea interpretativa utile concerne la verifica del rispetto, da parte di ciascuna delle figure coinvolte, dei doveri sulla stessa espressamente facenti capo agli stessi *ex lege*: sul punto si attende l'emanazione dei codici di condotta.

4. Le responsabilità penali dei DPO

Le fattispecie di reato connesse all'illegittimo trattamento di dati personali sono quelle previste dagli artt. 167 segg. - disciplinate dal Codice Privacy D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018 – (oltre – a titolo non esaustivo - all'art. 615 *ter* cod. pen. il reato di accesso abusivo ad un sistema informatico o telematico e l'art. 615 *quater* cod. pen. il reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, il danneggiamento di informazioni, dati, programmi informatici, art. 640 *bis* cod. pen., nonché di sistemi informatici, art. 640 *quater* cod. pen.), nonché i reati previsti dal c.d. Codice della Privacy (in particolare, pur in assenza di giurisprudenza formatasi in ordine ai reati "nuovi" 167 *bis*, 167 *ter*) inerenti il trattamento su larga scala, giunti dall'art. 15, comma 1, del D.lgs. 101 del 10.08.2018, si deve ritenere che

siano applicabili i criteri di formazione pretoria che sono stati sanciti interpretando l'art.167 cod. pen. vigente.

La norma in esame richiede, sotto il profilo soggettivo, il dolo specifico, non il semplice dolo generico, da parte di soggetti privati ed enti pubblici economici, consistente nell'intenzione di fare conseguire dal fatto di reato un profitto, per sé o per altri, oppure di arrecare un danno all'interessato (ovviamente nei trattamenti su larga scale tale precisazione manca vista la portata generale del danno).

La condanna per tale reato potrà essere inflitta solo ove si dimostri che il soggetto agente: 1) abbia agito con dolo specifico; 2) abbia agito con specifica intenzione di ricavare un profitto per sé o per altri; 3) abbia agito con specifica intenzione di cagionare un danno agli interessati.

È esclusa, pertanto, la responsabilità penale per colpa derivante da negligenza, imperizia o imprudenza dell'agente e la punibilità di questi reati è subordinata al verificarsi di un danno o alla finalità dell'acquisizione di un profitto, per sé o per altri. Tale distinzione può essere il fondamento della responsabilità penale del DPO: questo infatti agisce nell'interesse del titolare o del responsabile del trattamento, quindi ben potrebbe agire non per un profitto proprio per farlo conseguire ai propri designatori.

La responsabilità penale è personale, come noto riguarda solo le persone fisiche che hanno commesso o concorso a commettere il reato. Sotto tale profilo, la responsabilità del DPO potrebbe emergere tanto direttamente, quanto come concorso nel reato.

In assenza di autonome previsioni normative per individuare responsabilità specifiche del DPO, potrebbe essere utile confrontare la figura del responsabile protezione dei dati con quelle analoghe, già esistenti in altri ambiti specifici: si pensi al Responsabile del Servizio di Prevenzione e Protezione (R.S.P.P.) previsto dal D. Lgs. 81/2008 o l'Organismo di Vigilanza (OdV) previsto dal D.Lgs. 231/01.

Poiché l'art. 39 GDPR elenca in maniera non tassativa i compiti per i quali è designato (consulenza, sorveglianza, attribuzione delle responsabilità, sensibilizzazione e formazione del personale, emissione di pareri sulla valutazione di impatto e sorveglianza, cooperazione con l'autorità di controllo, contatto e

consultazioni preventive, valutazione dei rischi) non pare emergere un obbligo penalmente rilevante di svolgere tale attività acquisendo autonoma responsabilità penale. In sostanza, poiché il ruolo affidatogli sembrerebbe essere quello relativo ad una consulenza tecnica specializzata, la responsabilità penale sembrerebbe limitata al titolare e al responsabile.

Eppure, cooperando con il titolare della posizione di garanzia (ancora: titolare/responsabile) il DPO potrebbe essere ritenuto corresponsabile dei reati ai sensi dell'art. 40, comma 2, cod. pen. per la violazione dello specifico obbligo di impedire il verificarsi dell'evento dannoso.

Un profilo di responsabilità penale in capo al DPO permane nel caso in cui sia proprio la condotta del DPO a determinare l'evento dannoso o pericoloso connesso etiologicamente con la condotta.

Pertanto, nel caso in cui il DPO non abbia correttamente eseguito i compiti a lui attribuiti dal GDPR e abbia indotto il Titolare/Responsabile del trattamento dei dati ad omettere l'adozione di una doverosa misura organizzativa o di prevenzione, l'agente potrebbe risultare responsabile (ex art. 40, comma 2, cod. pen. al titolare/responsabile del trattamento) dell'evento derivato, essendo a lui astrattamente ascrivibile una responsabilità specifica, che potrebbe anche assumere caratteri di esclusività.

Infine, in forza del disposto dell'art. 39, comma 1, lett. d) ed e) del GDPR, si può configurare in capo al DPO una responsabilità in relazione alla correttezza delle comunicazioni e notificazioni effettuate all'Autorità Garante (art. 168 D.Lgs. 196/2003 come sostituito dall'art. 15 D.Lgs. 101/2018), salvo dimostrare un incolpevole affidamento alle informazioni ricevute o alle documentazioni inviate dai vertici aziendali o committenti (titolare/responsabile).

In particolare l'art. 24 bis D.Lgs. n. 231/01, che ha introdotto in Italia la cd. responsabilità amministrativa degli enti, si intitola "Delitti informatici e trattamento illecito dei dati". Esso punisce con sanzioni pecuniarie e in alcuni casi interdittive di varia natura applicate direttamente a carico dell'ente la violazione di alcune norme del vigente codice penale, che prevedono e puniscono ipotesi strettamente legate ad aspetti rientranti nella disciplina della privacy, intesa quale non solo quale tutela dei dati personali (reati di cui all'art. 167 segg.), bensì, di

tutti i dati, quali ad esempio – a titolo non esaustivo – l'accesso abusivo a sistemi informatici (art.615 *ter* cod. pen.), l'appropriazione e diffusione abusiva di codici di accesso (art. 615 *quater* cod. pen.), il danneggiamento di informazioni, dati, programmi informatici (art. 640 *bis* cod. pen.) nonché di sistemi informatici (art. 640 *quater* cod. pen.)

Appare evidente che si tratta di ipotesi delittuose che possono essere poste in essere laddove sia carente ovvero non dimostrabile una corretta ed adeguata tutela dei dati personali trattati in ambito aziendale mentre al contrario, una documentata osservanza della relativa normativa (tanto in materia 231 quanto soprattutto di privacy) potrebbe costituire un'esimente al riguardo.

Senza pretesa di esaustività della disamina di una complessa materia – qual è quella della responsabilità degli enti - si può affermare che la citata normativa ha ricompreso, nel novero dei reati cd. presupposto, anche alcune fattispecie strettamente legate ai profili della protezione dei dati, configurando per alcune figure di reato, un ulteriore profilo di punibilità a carico dell'ente, con elevate sanzioni pecuniarie (sino ad €.774.550,00) e, nelle ipotesi delittuose più gravi, anche interdittive dell'attività con confisca del profitto e pubblicazione della sentenza. Si tratta di un ulteriore e delicato aspetto, spesso non valutato con debito approfondimento da parte della aziende, che potrebbero vedere pregiudicata la loro stessa sopravvivenza nel caso non fossero in grado di dimostrare di aver attuato tempestivamente ai necessari interventi per adottare procedure idonee a comprovare, non solo sulla carta ma nella pratica effettiva, gli interventi necessari a limitare per quanto possibile, attraverso una completa analisi dei rischi e l'introduzione delle adeguate misure di sicurezza, incidenti di percorso nel trattamento dei dati.

CAPITOLO V
I "SUPERPOTERI" CELATI DEL DPO NELLA PUBBLICA AMMINISTRAZIONE

di Amedeo Pisanti

SOMMARIO: 1. L'obbligo di nomina del DPO tra ritardi cronici ed opportunità di rinnovamento. 2. Le procedure di gara per l'affidamento a soggetti esterni. 3. Procedimenti di scelta di dipendenti interni. 4. I requisiti richiesti nella P.A.: giurista, prima ancora che informatico. 5. Dal ruolo di supervisore a quello di controllore dei procedimenti amministrativi. 6. I necessari atti amministrativi di designazione ed il loro contenuto essenziale

1. L'obbligo di nomina del DPO tra ritardi cronici ed opportunità di rinnovamento

L'art. 37, par. 1, lett. a), del Regolamento Ue 2016/679 prevede che i titolari e i responsabili del trattamento designino un DPO "quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali".

Dunque, la nomina è dovuta in ambito pubblico, differentemente da quello privato, nel quale l'obbligo scatta solo in presenza di specifici requisiti posseduti dall'azienda.

Il GDPR, tuttavia, non fornisce la definizione di autorità pubblica o organismo pubblico e, come chiarito anche nelle Linee guida adottate in materia dal WP29[14], ne rimette l'individuazione al diritto nazionale applicabile[15].

In Italia sono obbligati alla designazione i soggetti che ricadevano nell'ambito di applicazione degli artt. 18-22 del D.Lgs. 169/2003, oggi abrogati dal D.Lgs. 101/2018, che stabilivano le regole generali per i trattamenti effettuati dai soggetti

[14] Il WP29 (acronimo di Working Party article 29, in italiano Gruppo articolo 29) è un organismo consultivo indipendente, composto da un rappresentante delle varie autorità nazionali, dal Garante europeo della protezione dei dati, nonché da un rappresentante della Commissione. Esso tra l'altro ha il potere di irrogare sanzioni, conoscere direttamente delle controversie in materia di dati personali, e di effettuare controlli preventivi e chiedere comunicazioni nel caso di trattamenti particolarmente delicati

[15] Al riguardo vedasi il par. 2.1.1., pag. 6, delle Linee guida sui responsabili della protezione dei dati adottate dal Gruppo Art. 29 (nelle note successive per brevità solo "Linee guida") il 13 dicembre 2016 ed emendate il 5 aprile 2017 (WP243 rev. 01), disponibili sul sito istituzionale Garante per la Protezione dei Dati Personali.

pubblici, quali le amministrazioni dello Stato, anche con ordinamento autonomo, gli enti pubblici non economici nazionali, regionali e locali, le regioni e gli enti locali, le università, le camere di commercio, industria, artigianato e agricoltura, le aziende del servizio sanitario nazionale, le autorità indipendenti.

A tali soggetti deve ritenersi possano essere affiancati anche quelli privati che esercitino funzioni pubbliche, come per esempio i concessionari di servizi pubblici, sebbene non sussista uno specifico obbligo.

Naturalmente ogni pubblica amministrazione, anche non rientrante nei soggetti sopra menzionati, su base volontaria può procedere alla designazione di un DPO ed in tal caso si applicano gli identici requisiti, in termini di criteri per la designazione, posizione e compiti, operanti quando la designazione è prevista come obbligatoria[16].

Malgrado il su descritto obbligo di legge di nomina del DPO in ambito pubblico, alla fine del 2018, secondo le stime di Federprivacy e de il Sole 24 Ore, solo una pubblica amministrazione locale su tre avrebbe provveduto ad effettuare la nomina del DPO, e la stragrande maggioranza non avrebbe neanche comunicato il nominativo tramite la procedura telematica messa a disposizione dal Garante per la Protezione dei Dati Personali.

In base ai dati disponibili, se da un lato gli enti locali, alla scadenza del 25 maggio 2018, hanno provveduto mediante apposito atto deliberativo di consiglio comunale all'approvazione formale dello schema di adeguamento al Regolamento Ue 679/2016, con la contestuale approvazione del registro dei trattamenti, molte amministrazioni non solo non avrebbero deliberato, ma addirittura neanche proceduto ad effettuare la nomina formale del DPO.

E' ciò costituisce la perdita di una grande opportunità di rinnovamento delle pubbliche amministrazioni di qualsiasi dimensione, dal piccolo comune

[16] Anche in caso di assenza del requisito soggettivo previsto dall'art. 37, par. 1, lett. a), del GDPR, il titolare o il responsabile del trattamento sono comunque tenuti alla designazione del DPO, ai sensi di quanto previsto dall'art. 37, par. 1, lett. b) e c), nel caso in cui le attività principali consistano: - in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala; - nel trattamento su larga scala di categorie di dati personali di cui all'art. 9 del GDPR o dei dati relativi alle condanne penali e a reati di cui all'art. 10 del GDPR. Con riferimento all'interpretazione delle espressioni "attività principali", "larga scala" e "monitoraggio regolare e sistematico" vedasi quanto riportato nelle Linee guida.

all'azienda sanitaria di grandi dimensioni, le quali, quando raggiungono la *compilance* in materia di *data protection*, hanno l'occasione per operare una revisione dei processi interni ed al tempo stesso adeguare anche la propria dotazione tecnologico-informatica, sia in termini hardware sia software, troppo spesso datata ed insicura, con grave compromissione della sicurezza dei dati dei cittadini, in molti casi anche di natura sensibile.

Tali ritardi, da un lato, sono dovuti ai cronici intoppi burocratici che troppo spesso ostacolano l'adeguamento normativo e, dall'altro, alle limitate risorse finanziarie tipiche dell'attuale congiuntura economica, la quale impone il contenimento della spesa pubblica anche a quegli enti che, non avendo personale disponibile per competenze e/o eccessivi carichi di lavoro per ricoprire il ruolo, non riescono ad indire procedure per l'affidamento all'esterno del servizio.

2. Le procedure di gara per l'affidamento a soggetti esterni

Infatti, anche nell'ambito pubblico, come in quello privato, l'incarico di DPO può essere ricoperto sia da un soggetto esterno[17] con competenze idonee, che da un dipendente interno, preferibilmente, come sarà illustrato nel paragrafo successivo, in posizione apicale e dotato di adeguata professionalità ed autonomia.

Per quanto riguarda l'affidamento esterno, esso si configura con un appalto di servizi e come tale soggiace alle norme del D.Lgs. 50/2016, non potendosi inquadrare come prestazione d'opera intellettuale ai sensi degli artt. 2222 e seguenti del codice civile. Ne consegue che le pubbliche amministrazioni sono tenute ad indire apposite procedure di evidenza pubblica, differenziate a seconda dell'importo dell'affidamento e non possono, naturalmente, come invece consentito al privato, operare *intuitus personae*.

Per la selezione di questo professionista, come per ogni appalto di servizi reso disponibile sui sistemi di *e-procurement*, l'art. 26, comma 3, della Legge 23/12/1999 n. 488 e l'art. 1 del D.L. 6 luglio 2012 n. 95, convertito con

[17] La funzione di DPO può essere esercitata anche in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna al titolare/responsabile del trattamento. In tal caso, come indicato nelle Linee guida, è indispensabile che ciascun soggetto appartenente alla persona giuridica operante quale DPO soddisfi tutti i requisiti richiesti dal GDPR. Cfr. sul punto le indicazioni del Gruppo Art. 29 riportate nel paragrafo 2.5., pag. 12, e nella domanda n. 7, pag. 24, delle Linee guida.

modificazioni in Legge 7 agosto 2012 n. 135 recante "Disposizioni urgenti per la revisione della spesa pubblica con invarianza dei servizi ai cittadini", dispongono la nullità dei relativi contratti stipulati dalle pubbliche amministrazioni in violazione degli obblighi di approvvigionamento del servizio, se non effettuato attraverso gli strumenti di acquisto messi a disposizione da Consip S.p.A. e dalle centrali di committenza regionali di riferimento.

Non è pertanto possibile affidare il servizio al di fuori delle piattaforme di *e-procurement*, che comunque oggi risultano ampiamente diffuse nel nostro ordinamento, in quanto Consip (società interamente partecipata dal Ministero delle Finanze) consente l'acquisto dei relativi sevizi attraverso il MEPA (Mercato Elettronico della Pubblica Amministrazione) sia in forma negoziata che diretta, mentre a livello locale si sono sviluppati sistemi analoghi, come ARCA SINtel della Regione Lombardia, START della Regione Toscana e CSI della Regione Piemonte.

Nonostante la pluralità di piattaforme di *e-procurement* e la disponibilità del servizio offerta da parte di fornitori, nella forma di società o di liberi professionisti, si registrano casi di amministrazioni che continuano a fare ricorso ai sistemi tradizionali, per altro poco trasparenti, oltreché *contra legem*, tanto che la discrezionalità spesso si trasforma in vera e propria arbitrarietà.

In tale ambito si registra già un primo importante e recentissimo intervento della magistratura amministrativa, la quale sotto il profilo del rispetto del principio di trasparenza imposto dal D.Lgs. 50/2016 ha stabilito che "è illegittimo il provvedimento con il quale la stazione appaltante avvia la procedura per l'affidamento, attraverso una procedura negoziata, del servizio di responsabile della protezione dei dati personali previsto dall'art. 37 del Regolamento Ue 2016/679, se non è stata data prima pubblicità alla fase preliminare di esplorazione del mercato, così da precludere la più ampia partecipazione degli operatori e la selezione di soggetti specializzati in materia di protezione dei dati"[18].

[18] T.A.R. Friuli Venezia Giulia – sede di Trieste, sezione I, sentenza n. 252 del 18/07/2018.

Chiarite le modalità attraverso le quale deve avvenire *ex lege* l'affidamento del servizio, appare importante definire il perimetro dei requisiti professionali che dovrebbe avere il DPO.

Infatti, sul versante dell'affidamento del servizio all'esterno, occorre definire requisiti che non siano eccessivamente penalizzanti per la *par condicio* dei concorrenti alla procedura di evidenza pubblica ed al tempo stesso siano idonei ad assicurare la scelta di un soggetto dotato di adeguata professionalità e competenza, che possa garantire l'esecuzione di una prestazione coerente con le dimensioni e la complessità dell'organizzazione dell'ente.

Sotto tale profilo si è pronunciato recentemente il T.A.R. Friuli Venezia Giulia – sede di Trieste, che, con riferimento alla certificazione ISO richiesta come requisito di accesso per il confronto concorrenziale previsto dalla *lex specialis* di una gara bandita da un ente locale, ha stabilito che "la certificazione di Auditor/Lead Auditor ISO/IEC/27001 non costituisce un titolo abilitante ai fini dell'assunzione e dello svolgimento delle funzioni di responsabile della sicurezza dei dati, nell'alveo della disciplina introdotta dal GDPR, dovendosi considerare che la norma ISO 27001 trova prevalente applicazione nell'ambito dell'attività di impresa, e che la stessa, per quanto potenzialmente estensibile all'attività delle pubbliche amministrazioni, fa pur sempre salva l'applicazione delle disposizioni speciali (euro-unitarie e nazionali) in materia di tutela dei dati personali e della riservatezza. Ne consegue che la certificazione indicata, di per sé, non può costituire requisito di ammissione alla selezione per l'affidamento dell'incarico di responsabile della protezione dei dati, trattandosi di un mero titolo curriculare (certamente valutabile in sede di giudizio sulle posizioni dei singoli candidati), ma non anche di un titolo formativo o abilitante, come tale idoneo ad assurgere a requisito di accesso"[19].

3. Procedimenti di scelta di dipendenti interni

Per quanto attiene, invece, la selezione di una risorsa interna all'amministrazione si pone il problema di definire quale qualifica debba rivestire il dipendente

[19] T.A.R. Friuli Venezia Giulia – sede di Trieste, sezione I, sentenza n. 287 del 13/09/2018.

pubblico assegnatario dell'incarico di DPO: nell'ambito del lavoro alle dipendente della pubblica amministrazione, infatti, il D.Lgs. 165/2001 distingue funzionari e dirigenti, questi ultimi con diversi gradi di responsabilità.

Invero, il GDPR non fornisce specifiche indicazioni al riguardo e pertanto risulta opportuno, in primo luogo, valutare se il complesso dei compiti assegnati siano o meno compatibili con le mansioni ordinariamente affidate ai dipendenti con qualifica non dirigenziale. Il DPO, difatti, è chiamato ad assumere compiti aventi rilevanza interna, come consulenze, pareri, sorveglianza sul rispetto delle disposizioni, ed esterna, quali la cooperazione con l'autorità di controllo e contatto con gli interessati in relazione all'esercizio dei propri diritti.

In merito, l'art. 38, par. 3, del GDPR[20] fissa alcune garanzie essenziali per consentire ai DPO di operare con un grado sufficiente di autonomia all'interno dell'organizzazione. In particolare, come si legge nella norma, occorre assicurare che il DPO "non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti". Il considerando 97 aggiunge che i DPO "dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente". Ciò significa, come chiarito nelle Linee guida adottate dal WP29, che "il DPO, nell'esecuzione dei compiti attribuitigli ai sensi dell'art. 39, non deve ricevere istruzioni sull'approccio da seguire nel caso

[20] Art. 38 del Regolamento Ue 679/2016: il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.
4 Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.
6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

specifico: quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo. Né deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati".

Inoltre, sempre ai sensi dell'art. 38, par. 3, del GDPR, il DPO "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.

Per quanto sopra, nel caso la scelta ricada su un dipendente interno, appare preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, 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.

Visto il profilo di elevata responsabilità, come sopra delineato, derivante dalla molteplicità di compiti e funzioni rivestiti dal DPO, soprattutto nelle pubbliche amministrazioni articolate in una vasta pluralità di uffici e a servizio di un'ampia platea di cittadini, si pone anche il problema di stabilire se ed in che termini l'incaricato debba essere dotato di un proprio ufficio, con eventuale assegnazione di personale dedicato.

Il Regolamento Ue 679/2016 prevede, all'art. 38, par. 2, che "il titolare del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'art. 39, fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica".

Ne discende che, in relazione alla complessità (amministrativa e tecnologica) dei trattamenti e dell'organizzazione, occorrerà valutare attentamente se una sola persona possa essere sufficiente a svolgere il complesso dei compiti affidati. Come riportato anche nelle Linee guida del WP29, in linea di principio, quanto più aumentano complessità e/o sensibilità dei trattamenti, tanto maggiori devono

essere le risorse messe a disposizione del DPO. La funzione "protezione dati" deve poter operare con efficienza e contare su risorse sufficienti in proporzione al trattamento svolto[21].

All'esito di questa analisi si potrà valutare quindi l'opportunità/necessità di istituire un apposito ufficio, al quale eventualmente destinare le risorse necessarie allo svolgimento dei compiti stabiliti. Ad ogni modo, ove sia costituito un apposito ufficio, è comunque necessario che venga sempre individuata la persona fisica che riveste il ruolo di DPO mediante un apposito atto di designazione (come sarà illustrato nel successivo paragrafo 6).

4. I requisiti richiesti nella P.A.: giurista, prima ancora che informatico

Come accennato nel paragrafo 2 il tema dei requisiti professionali del DPO in ambito pubblico solo recentemente è stato affrontato dalla giurisprudenza, seppur soltanto sotto il profilo della scelta di un soggetto esterno.

Nel tempo si sono diffusi sistemi di attestazione delle competenze professionali offerti da enti certificatori in modo volontario. Tali certificazioni (che non rientrano tra quelle disciplinate dall'art. 42 del GDPR[22]) sono rilasciate anche

[21] Cfr. Linee guida, paragrafo 3.2., pag. 15

[22] Art. 42 del Regolamento Ue 679/2016: 1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese.
2. Oltre all'adesione dei titolari del trattamento o responsabili del trattamento soggetti al presente regolamento, i meccanismi, i sigilli o i marchi approvati ai sensi del paragrafo 5 del presente articolo possono essere istituiti al fine di dimostrare la previsione di garanzie appropriate da parte dei titolari del trattamento o responsabili del trattamento non soggetti al presente regolamento ai sensi dell'articolo 3, nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 46, paragrafo 2, lettera f). Detti titolari del trattamento o responsabili del trattamento assumono l'impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati. (1)
3. La certificazione è volontaria e accessibile tramite una procedura trasparente.
4. La certificazione ai sensi del presente articolo non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti a norma degli articoli 55 o 56.
5. La certificazione ai sensi del presente articolo è rilasciata dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente in base ai criteri approvati da tale autorità di controllo competente ai sensi dell'articolo 58, paragrafo 3, o dal comitato, ai sensi dell'articolo 63. Ove i criteri siano approvati dal comitato, ciò può risultare in una certificazione comune, il sigillo

all’esito della partecipazione ad attività formative e al controllo dell’apprendimento[23].

Esse, 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 DPO né, allo stato, sono idonee a sostituire il giudizio rimesso alle amministrazioni nella valutazione dei requisiti necessari per svolgere i compiti previsti dall’art. 39 del GDPR, come ha chiarito il Garante per la Protezione dei Dati Personali[24].

Se nel settore privato la scelta del DPO è riservata all’esclusiva discrezionalità dell’azienda, che può optare per il fornitore esterno che preferisce o selezionare tra i suoi dipendenti come meglio crede quello ritenuto più idoneo sulla base di un giudizio insindacabile, negli enti pubblici essa è sottoposta alla rigorosa osservanza delle norme in tema di appalti e personale dipendente. Infatti, da un lato il D.Lgs. 50/2016 impone il rispetto dei principi irrinunciabili di economicità, efficacia, tempestività e correttezza in tema di affidamenti di appalti di servizi e dall’altro il D.Lgs. 165/2001 non consente di prescindere dai ruoli e funzione del personale in cui si articola l’organizzazione del singolo ente.

---

europeo per la protezione dei dati.

6. Il titolare del trattamento o il responsabile del trattamento che sottopone il trattamento effettuato al meccanismo di certificazione fornisce all’organismo di certificazione di cui all’articolo 43 o, ove applicabile, all’autorità di controllo competente tutte le informazioni e l’accesso alle attività di trattamento necessarie a espletare la procedura di certificazione.

7. La certificazione è rilasciata al titolare del trattamento o responsabile del trattamento per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i criteri pertinenti. La certificazione è revocata, se del caso, dagli organismi di certificazione di cui all’articolo 43 o dall’autorità di controllo competente, a seconda dei casi, qualora non siano o non siano più soddisfatti i criteri per la certificazione. (1)

8. Il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato.

[23] Sul tema della certificazione il 18 luglio 2017 è stato pubblicato sul sito del Garante per la Protezione dei Dati Personali (doc. web n. 6621723) un comunicato con il quale il Garante e ACCREDIA (l’Ente unico nazionale di accreditamento designato dal Governo italiano) hanno ritenuto necessario sottolineare - al fine di indirizzare correttamente le attività svolte dai soggetti a vario titolo interessati in questo ambito - che “al momento le certificazioni di persone, nonché quelle emesse in materia di privacy o *data protection* eventualmente rilasciate in Italia, sebbene possano costituire una garanzia e atto di diligenza verso le parti interessate dell’adozione volontaria di un sistema di analisi e controllo dei principi e delle norme di riferimento, a legislazione vigente non possono definirsi "conformi agli artt. 42 e 43 del regolamento 2016/679", poiché devono ancora essere determinati i "requisiti aggiuntivi" ai fini dell’accreditamento degli organismi di certificazione e i criteri specifici di certificazione.

[24] Cfr. nuove FAQ sul Responsabile della Protezione dei dati (RPD) in ambito pubblico (in aggiunta a quelle adottate dal Gruppo Art. 29 in Allegato alle Linee guida sul RPD).

La sentenza del TAR Friuli Venezia Giulia – sede di Trieste n. 287/2018, richiamata sopra nel paragrafo 2, costituisce anche un importante precedente (valido pure nei casi di risorsa interna all'ente), che delinea il profilo professionale del DPO nella pubblica amministrazione, sradicando ogni fantasiosa e futura diversa interpretazione ed indentificandolo quale soggetto con prevalenti competenze di natura giuridica, prima ancora che tecnico-informatiche.

I giudici friulani, infatti, hanno chiarito che "in sede di conferimento, ai sensi dell'art. 7, D.Lgs. n. 165 del 2001, dell'incarico di responsabile della protezione dei dati personali, la certificazione di Auditor/Lead Auditor per i Sistemi di Gestione per la Sicurezza delle Informazioni, secondo la norma ISO/IEC/27001, non può costituire titolo abilitante ai fini dell'assunzione e dello svolgimento delle relative funzioni, il cui esercizio presuppone la minuziosa conoscenza e l'applicazione del Regolamento Ue 2016/679 e della complessiva disciplina di settore, (né tanto meno assurgere a titolo equipollente al richiesto diploma di laurea), proprio perché essa non coglie (o non coglie appieno) la specifica funzione di garanzia insita nell'incarico conferito, il cui precipuo oggetto non è costituito dalla predisposizione dei meccanismi volti ad incrementare i livelli di efficienza e di sicurezza nella gestione delle informazioni ma attiene semmai, come rilevato nel ricorso, alla tutela del diritto fondamentale dell'individuo alla protezione dei dati personali indipendentemente dalle modalità della loro propagazione e dalle forme, ancorché lecite, di utilizzo"[25].

[25] T.A.R. Friuli Venezia Giulia – sede di Trieste, sezione I, sentenza n. 287 del 13/09/2018 con la quale il tribunale amministrativo ha annullato una procedura concorsuale finalizzata alla nomina di in DPO in ambito pubblico precisando che "Venendo al merito dell'impugnazione, ritiene il Collegio che essa sia manifestamente fondata in relazione alla contestata individuazione della certificazione di Auditor/Lead Auditor ISO/IEC/27001 quale requisito di ammissione alla procedura selettiva (censura n. 1.1, introdotta nel ricorso, reiterata nei motivi aggiunti al n. 3).
Sul punto, va rilevato che la predetta certificazione non costituisce, come eccepito dal ricorrente, un titolo abilitante ai fini dell'assunzione e dello svolgimento delle funzioni di responsabile della sicurezza dei dati, nell'alveo della disciplina introdotta dal GDPR, dovendosi considerare che: da un lato, la norma ISO 27001 trova prevalente applicazione nell'ambito dell'attività di impresa (basti rilevare che i riferimenti rivolti ad essa, dal legislatore nazionale e dall'ordinamento euro-unitario, attengono essenzialmente ai requisiti degli operatori economici, come ad esempio avviene nel caso dell'art. 93, comma 7, D.Lgs. n. 50 del 2016, in tema di garanzie per la partecipazione alle procedure di affidamento nei settori ordinari); dall'altro lato, la medesima norma, per quanto potenzialmente estensibile all'attività delle pubbliche amministrazioni, fa pur sempre salva l'applicazione delle disposizioni speciali (euro-unitarie e nazionali) in materia di tutela dei dati personali e della riservatezza (punto 18 "conformità" della citata norma ISO; cfr. in particolare: 18.1.1 e 18.1.4), sicché la minuziosa conoscenza e l'applicazione della disciplina di

5. Dal ruolo di supervisore a quello di controllore dei procedimenti amministrativi

La normativa vigente consente l'assegnazione al DPO di ulteriori compiti e funzioni, a condizione che non diano adito a un conflitto di interessi (art. 38, par. 6) e che gli consentano di avere comunque a disposizione il tempo sufficiente per l'espletamento dei compiti previsti dalla legge (art. 38, par. 2).

A seconda della natura dei trattamenti e delle attività e dimensioni della struttura del titolare o del responsabile, le eventuali ulteriori incombenze attribuite al DPO, come suggerito dal Garante per la Protezione dei Dati Personali, non dovrebbero pertanto sottrarre allo stesso il tempo necessario per adempiere alle relative responsabilità.

In linea di principio, è quindi ragionevole che negli enti pubblici di grandi dimensioni, con trattamenti di dati personali di particolare complessità e sensibilità, non vengano assegnate al DPO ulteriori responsabilità (si pensi, ad esempio, alle amministrazioni centrali, alle agenzie, agli istituti previdenziali, nonché alle Regioni e alle ASL).

In tale quadro, ad esempio, avuto riguardo, caso per caso, alla specifica struttura organizzativa, alla dimensione e alle attività del singolo titolare o responsabile, l'attribuzione delle funzioni di DPO al responsabile per la prevenzione della corruzione e per la trasparenza, figura espressamente prevista dalla legge n.190/2012, considerata la molteplicità degli adempimenti che incombono su tale figura, potrebbe rischiare di creare un cumulo di impegni tali da incidere negativamente sull'effettività dello svolgimento dei compiti.

Un tema particolarmente delicato, poi, in ambito pubblico, riguarda i possibili conflitti di interessi in cui possa incorrere il DPO. Infatti, le ulteriori funzioni allo stesso assegnate non devono consentirgli di definire le finalità e modalità del trattamento dei dati.

Ciò si traduce nella possibilità che, oltre che per i casi di ruoli manageriali di vertice, possano sussistere situazioni di conflitto di interesse rispetto a figure

---

settore restano, indipendentemente dal possesso o meno della certificazione in parola, il nucleo essenziale ed irriducibile della figura professionale ricercata mediante la procedura selettiva intrapresa dall'Azienda, il cui profilo, per le considerazioni anzidette, non può che qualificarsi come eminentemente giuridico".

apicali dell'amministrazione investite di capacità decisionali in ordine alle finalità e ai mezzi del trattamento di dati personali posti in essere dall'ente pubblico, ivi compreso, ad esempio, il responsabile dei Sistemi informativi (chiamato ad individuare le misure di sicurezza necessarie), ovvero quello dell'Ufficio di statistica (deputato a definire le caratteristiche e le metodologie del trattamento dei dati personali utilizzati a fini statistici).

Riguardo agli ulteriori compiti e funzioni in capo al DPO, particolare attenzione, dunque, andrebbe prestata nei casi di unico DPO tra molteplici autorità pubbliche e organismi pubblici, nonché in quelli di DPO esterno, qualora questi svolga ulteriori compiti che comportino situazioni di conflitto di interesse oppure quando non sia in grado di adempiere in modo efficiente alle sue funzioni. In questi casi, nell'atto di designazione o nel contratto di servizio, l'aggiudicatario dovrà fornire opportune garanzie per assicurare efficienza e correttezza e prevenire conflitti di interesse.

Alcune organizzazioni complesse hanno richiesto al Garante per la Protezione dei Dati Personali di valutare la possibilità di designare più DPO, ma questi ha segnalato che in linea di massima l'unicità di questa figura è una condizione necessaria per evitare il rischio di sovrapposizioni o incertezze sulle responsabilità, sia con riferimento all'ambito interno all'ente, sia con riferimento a quello esterno, e pertanto occorre che questa sia sempre assicurata.

Nulla osta, invece, secondo il Garante per la Protezione dei Dati Personali, all'individuazione di più figure di supporto, con riferimento a settori o ambiti territoriali diversi, anche dislocate presso diverse articolazioni organizzative dell'amministrazione, che facciano però riferimento a un unico soggetto responsabile, sia che la scelta ricada su un soggetto interno, sia che questa ricada su uno esterno.

Infatti, in relazione alla particolare eterogeneità dei trattamenti di dati personali effettuati (in rapporto, ad esempio, all'effettuazione di trattamenti soggetti a basi giuridiche diverse in ambito di prevenzione, indagine, accertamento e perseguimento di reati) ovvero della complessità della struttura organizzativa dell'ente (talvolta molto ramificata a livello territoriale) può risultare opportuno individuare specifici "referenti" del DPO, che potrebbero svolgere un ruolo di

supporto e raccordo, sulla base di precise istruzioni da questi impartite, anche, se del caso, operando quali componenti del suo gruppo di lavoro.

In definitiva, l'articolazione complessa e radicata di molti enti, l'ampiezza della platea di cittadini coinvolti dai provvedimenti da questi assunti e soprattutto la natura degli interessi stessi che vengono messi in gioco davanti alla pubblica amministrazione pone chi, come il DPO, è deputato a sorvegliarne la conformità dei procedimenti amministrativi alle nome in materia di protezione dei dati in una posizione di fatto di controllo dei procedimenti stessi.

6. I necessari atti amministrativi di designazione ed il loro contenuto essenziale

Una volta selezionato il DPO, l'ente pubblico deve adottare un apposito atto amministrativo di nomina avente efficacia costitutiva. Tanto si ricava anche dall'art. 37, par. 1, del GDPR, che prevede che il titolare e il responsabile del trattamento designino il DPO.

Nel caso in cui la scelta del DPO ricada su una professionalità interna all'ente, occorre formalizzare un apposito atto di designazione a "Responsabile per la protezione dei dati". In caso, invece, di ricorso a soggetti esterni all'ente, la designazione costituirà parte integrante dell'apposito contratto d'appalto redatto in base a quanto previsto dal citato art. 37 del RGPD[26].

Indipendentemente dalla natura e dalla forma dell'atto utilizzato, è necessario che nello stesso sia individuato in maniera inequivocabile il soggetto che opererà come DPO, riportandone espressamente le generalità[27], i compiti, eventualmente anche ulteriori a quelli previsti dall'art. 39 del GDPR, e le funzioni che questi sarà

[26] Sul sito web del Garante per la Protezione dei Dati Personali è disponibile anche uno schema di atto di designazione predisposto per facilitare le amministrazioni nell'adempimento (doc web 7322273).

[27] Secondo quanto precisato nelle Linee guida, se la funzione di DPO è svolta da un fornitore esterno di servizi, i compiti stabiliti per il DPO potranno essere assolti efficacemente da un team operante sotto l'autorità di un contatto principale designato e "responsabile" per il singolo cliente. In particolare, «per favorire una corretta e trasparente organizzazione interna e prevenire conflitti di interesse a carico dei componenti il team DPO, si raccomanda di procedere a una chiara ripartizione dei compiti all'interno del team DPO e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente. Sarà utile, in via generale, inserire specifiche disposizioni in merito nel contratto di servizi» (cfr. par. 2.5., pag. 12).

chiamato a svolgere in ausilio al titolare/responsabile del trattamento, in conformità a quanto previsto dal quadro normativo di riferimento.

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

Nell'atto di designazione o nel contratto di servizi è opportuno che risultino anche le motivazioni che hanno indotto l'ente a individuare, nella persona fisica selezionata, il proprio DPO, al fine di consentire la verifica del rispetto dei requisiti previsti dall'art. 37, par. 5 del GDPR, 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 e di buon amministrazione, costituisce anche elemento di valutazione del rispetto del principio cardine di responsabilizzazione dettato dal Regolamento Ue 679/2016.

Ma il processo post selettivo non termina qui. Un'ulteriore normativa, infatti, interviene a differenziare gli adempimenti conseguenti la nomina del DPO in ambito pubblico, rispetto a quello privato. Si tratta del D.Lgs. n. 33/2013 recante "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni"

Una volta individuato, infatti, il titolare o il responsabile del trattamento è tenuto a indicare, nell'informativa fornita agli interessati, i dati di contatto del DPO, pubblicando gli stessi anche sul siti web dell'amministrazione e a comunicarli al Garante (art. 37, par. 7). Per quanto attiene al sito web, può risultare opportuno inserire i riferimenti del DPO nella sezione "amministrazione trasparente", oltre che nella sezione "privacy" eventualmente già presente ai sensi del D.Lgs n. 33/2013.

Come chiarito nelle Linee guida del WP29, in base all'art. 37, par. 7, non è necessario, anche se potrebbe costituire una buona prassi in ambito pubblico, pubblicare anche il nominativo del DPO, mentre occorre che sia comunicato al Garante per la Protezione dei Dati Personali per agevolare i contatti con

l’Autorità. Resta invece fermo l’obbligo di comunicare il nominativo agli interessati in caso di violazione dei dati personali (art. 33, par. 3, lett. b).

Nel contesto legislativo sopra delineato, nel quale le norme in materia di protezione dei dati si intrecciano con quelle che governano i superiori interessi tutelati dalla pubblica amministrazione, il ruolo del *Data Protection Officer* attrae in se una molteplicità di poteri, che, seppur non espressamente attribuitigli, vanno ben al di là del compito di sorveglianza tradizionalmente svolto in ambito privato.

Infatti, per un verso, per l’ampiezza del raggio operativo d’azione riconosciutogli e, per un altro verso, per la delicatezza e complessità dei compiti attribuitigli, svolti per di più in una posizione di completa autonomia, diversamente dal settore privato, ove, tanto in qualità di dipendente quanto in quella di esperto esterno, esegue una prestazione tutto sommato consulenziale, in ambito pubblico il DPO finisce con l’assumere di fatto un ruolo di vero controllore dei procedimenti amministrativi, con l’attribuzione di poteri sostanziali, che probabilmente sono andati oltre la volontà del legislatore.

CAPITOLO VI
LA FORMALIZZAZIONE DELL'INCARICO, I CONTENUTI DELLE DELEGHE E LO SVOLGIMENTO DELLA MANSIONE

di Sara Bassolamento

SOMMARIO: 1. La formalizzazione dell'incarico. 2. Comunicazione del nominativo del Responsabile della Protezione dati al Garante. 3. Considerazioni conclusive. Allegato A – Schema di atto di designazione del Responsabile della Protezione dei Dati (RPD) ai sensi dell'art. 37 del Regolamento UE 2016/679. Allegato B. Lettera d'incarico professionale per lo svolgimento dell'incarico di D.P.O. (Data Protection Officer).ART. 37 REG. UE 2016/679.

1. La formalizzazione dell'incarico

Il GDPR richiede, rispetto alle precedenti normative in tema di privacy, una maggiore attenzione verso il tema della protezione dei dati personali proprio perché, a monte, vi è la tutela di interessi fondamentali ma con un cambio di paradigma che possiamo individuare, in primo luogo, nel principio di *accountability* (o, nella versione italiana, nel principio di responsabilizzazione).

La designazione a *Data Protection Officer* viene formalizzata con apposito atto o come parte integrante del contratto di servizi. In entrambi i casi deve essere individuato in maniera inequivocabile il soggetto che opererà come tale e indicate le generalità, i compiti e le funzioni da svolgere in ausilio al Titolare/Responsabile.

Questi ultimi sono inoltre tenuti ad illustrare le motivazioni che hanno indotto la scelta della determinata persona fisica selezionata, anche al fine di verificarne i requisiti ed il processo di selezione. Tale attività, oltre a rappresentare una buona prassi di condotta è indice di trasparenza e costituisce, ancora una volta, elemento di valutazione del rispetto del principio della "*accountability*".

Nel settore pubblico la normativa appare chiara nel delineare un obbligo di designazione e nel lasciare spazio alla condivisione di un unico DPO, naturalmente se tale condivisione risulti misura conforme alla struttura organizzativa e dimensionale dell'ente. Nel caso che l'ente pubblico dovesse rivolgersi a soggetti esterni, si dovrà considerare l'obbligo di procedere a selezioni e mediante procedure di evidenza pubblica ai sensi del D.lgs. n. 50/2016.

Nella lettera di incarico, invece, sarà opportuno specificare le funzioni del DPO nominato, le modalità di svolgimento dell'incarico professionale, la durata dell'incarico, revoca dell'incarico, determinazione del compenso e modalità di pagamento, possibilità per il DPO di utilizzare i professionisti, consulenti ed esperti esterni al DPO e modalità di tutela della segretezza.

In particolare, nella lettera di incarico al DPO andrà indicato che, nel rispetto della normativa, egli dovrà:

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 regolamento 2016/679 nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

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'art. 35;

d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nella lettera di incarico è opportuno precisare anche che il DPO, per l'espletamento dell'incarico, potrà avvalersi di un team di tecnici e professionisti in possesso delle professionalità necessarie per lo svolgimento delle funzioni oggetto del presente incarico i quali potranno operare anche disgiuntamente con riferimento alle fasi di svolgimento dei servizi consulenza ed assistenza.

È consigliabile, infine, specificare che le attività oggetto dell'incarico saranno svolte con accessi (previo accordo sulla data dell'incontro) presso la società per analisi, verifiche documentali, colloqui con il management e interviste alle varie funzioni aziendali in base alle esigenze riscontrate e presso la sede del DPO per

studio di atti ed esame dei documenti, nonché per ricerche giuridiche e tecniche.

Relativamente agli obblighi della società di assicurare la necessaria collaborazione dei soggetti facenti parte dell'organizzazione in tutte le fasi di svolgimento dell'attività oggetto dell'incarico e di assicurare la messa a disposizione di tutta la documentazione necessaria per lo svolgimento delle attività oggetto dell'incarico, appare opportuno indicare che andranno messi a disposizione del Responsabile della protezione dei dati anche le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

Preme infine ricordare che, come anche chiarito nelle recenti linee giuda, il DPO non potrà rispondere personalmente della non conformità dell'organizzazione al regolamento europeo, responsabilità dirette che ricadono esclusivamente sul titolare e sul responsabile. Il DPO tuttavia assume responsabilità contrattuali nei confronti del titolare/responsabile del trattamento.

Per i trattamenti effettuati da un'autorità pubblica, eccettuate le autorità giurisdizionali o autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali, o per i trattamenti effettuati nel settore privato da un titolare del trattamento le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, o ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati, il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento. Nel settore privato le attività principali del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria. Il livello necessario di conoscenza specialistica dovrebbe essere determinato in particolare in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento. Tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente.

È opportuno, infine, valutare se il complesso dei compiti assegnati al DPO – aventi rilevanza interna (consulenza, pareri, sorveglianza sul rispetto delle disposizioni) ed esterna (cooperazione con l'autorità di controllo e contatto con gli interessati in relazione all'esercizio dei propri diritti) – siano (o meno) compatibili con le mansioni ordinariamente affidate ai dipendenti con qualifica non dirigenziale.

In merito, l'art. 38, par. 3, del GDPR fissa alcune garanzie essenziali per consentire ai DPO di operare con un grado sufficiente di autonomia all'interno dell'organizzazione. In particolare, occorre assicurare che il DPO *"non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti"*. Il considerando 97 aggiunge che i DPO "*dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente"*. Ciò significa, come chiarito nelle Linee guida, che *"il DPO, nell'esecuzione dei compiti attribuitigli ai sensi dell'art. 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico – quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo. Né deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati"*.

2. Comunicazione del nominativo del Responsabile della Protezione dati al Garante.

In base all'art. 37, paragrafo 7 del Regolamento UE/2016/679 occorre che i soggetti pubblici e privati comunichino al Garante per la protezione dei dati personali il nominativo del Responsabile della Protezione dei dati, se designato.

Questa disposizione mira a garantire che le autorità di controllo possano contattare il Responsabile della Protezione dei Dati in modo facile e diretto, come chiarito nelle Linee guida sui Responsabili della Protezione dei Dati (RPD) adottate dal Gruppo Articolo 29 (WP 243 rev. 01 - punto 2.6).

Si ricorda, infatti, che in base all'art. 39, paragrafo 1, lettera e) del Regolamento, il Responsabile della Protezione dei Dati funge da punto di contatto fra il singolo ente o azienda e il Garante.

Sul sito ufficiale del Garante della Privacy è stata resa disponibile la procedura telematica che consente alle aziende interessate all'adempimento di effettuare la comunicazione dei dati di contatto del Responsabile della Protezione dei dati (DPO).

Tale procedura è l'unica che può essere utilizzata per l'invio dei dati di contatto del Responsabile della protezione dei dati e non potranno essere prese in considerazione le comunicazioni effettuate attraverso diversi canali di contatto con il Garante (es. e-mail, posta, ecc.).

La comunicazione deve essere effettuata dal Legale Rappresentante del soggetto Titolare/Responsabile del trattamento dei dati, o da un suo delegato.

Orbene nella Sezione A – andranno inseriti i dati del soggetto che effettua la comunicazione (Cognome, Nome e l'indirizzo e-mail del soggetto che provvede ad effettuare la comunicazione). Qualora la comunicazione venga effettuata su delega del rappresentante legale è necessario indicare il Cognome ed il Nome del soggetto delegante.

Per proseguire con la compilazione del modello di comunicazione è necessario prendere visione dell'informativa relativa al trattamento dei dati personali.

Nella sezione B andranno indicate alcune informazioni del Titolare/Responsabile che effettua la comunicazione. Per i soggetti che risultano essere censiti in uno degli indici previsti dagli art. 6-bis e art. 6-ter del CAD, è obbligatorio fornire l'indirizzo PEC, mentre il conferimento dell'indirizzo e-mail è facoltativo. Per i soggetti che non risultano essere censiti in uno dei due citati indici, o che operano in un altro Stato, è obbligatorio fornire un valido indirizzo e-mail, mentre il conferimento della PEC è facoltativo.

Nella sezione B1 – Gruppi imprenditoriali è necessario indicare se il Titolare/Responsabile che effettua la comunicazione fa parte di un gruppo imprenditoriale che si è avvalso della nomina di un unico Responsabile della protezione dei dati, secondo quanto previsto dall'art. 37, par. 2, del GDPR.

In tal caso, se il soggetto che effettua la comunicazione è la società controllante (del gruppo imprenditoriale) è necessario selezionare l'apposita spunta. Se il soggetto che effettua la comunicazione, invece, è una società controllata è necessario indicare le informazioni che permettano di risalire a quanto già

comunicato dalla società controllante.

Saranno pertanto richiesti:

- il C.F./P.I. della società controllante ed il numero di protocollo assegnato alla comunicazione mediante la quale la controllante ha comunicato il RPD, ovvero - la denominazione della società controllante e lo Stato presso la cui Autorità è stata effettuata la comunicazione del RPD.

Qualora il soggetto che effettua la comunicazione faccia parte di un gruppo imprenditoriale che si è avvalso della nomina di un unico Responsabile della protezione dei dati, secondo quanto previsto dall'art. 37, par. 2, del RGPD, vi è la possibilità di fornire i riferimenti di un altro Responsabile della protezione dei dati facilmente raggiungibile da ciascun stabilimento ex art. 37, par. 2 del RGPD. In tal caso, si passa alla compilazione della sezione C.

Nella Sezione C, dedicata ai dati del "*Responsabile della protezione dei dati*" (al punto 1), è necessario indicare se il RPD designato è un soggetto interno o esterno, al fine di individuare di quale possibilità prevista dall'art. 37, par. 6 si è avvalso il soggetto Titolare o Responsabile che sta effettuando la Comunicazione.

Qualora il RPD sia esterno, è necessario indicare la natura del soggetto (Persona fisica o giuridica) con cui il Titolare o Responsabile del trattamento ha stipulato un contratto di servizio: nel caso di persona giuridica, sarà necessario fornire le informazioni di cui al punto 3, nel caso di persona fisica sarà necessario fornire le informazioni di cui al punto 4.

Al punto 4 devono essere riportati i dati della persona fisica designata quale RPD, oppure del soggetto individuato quale referente per il Titolare/Responsabile nel caso si tratti di RPD esterno operante sulla base di contratto di servizi sottoscritto con una persona giuridica.

Al punto 5 vanno inseriti i dati di contatto.

Nella sezione D relativa alla "*Pubblicazione dei dati di contatto del RPD*", vanno indicate le modalità adottate dal Titolare o dal Responsabile del trattamento al fine di pubblicare i dati di contatto del RPD.

Al termine della fase di inserimento di tutte le informazioni richieste, il soggetto che effettua la comunicazione riceverà una e-mail contenente le istruzioni per completare la procedura. In particolare, bisognerà scaricare un file che dovrà

essere sottoscritto con firma digitale (o firma elettronica qualificata) in formato CAdES (file con estensione p7m) e successivamente caricato in una specifica sezione della piattaforma applicativa. La procedura di caricamento deve essere completata entro 48 ore dalla ricezione della mail contenente le istruzioni.

Per l'apposizione della firma è necessario utilizzare un dispositivo di firma digitale disponibile presso uno dei certificatori accreditati.

L'invio del file firmato digitalmente costituisce l'invio di comunicazione al Garante per la protezione dei dati personali, ed è identificato da un ID provvisorio di comunicazione.

La comunicazione così ricevuta sarà analizzata sotto il profilo formale, verificando in particolare la validità della firma digitale e la perfetta corrispondenza fra il file firmato e quello già inviato via e-mail. A tal fine, si rappresenta che la minima modifica al file ricevuto comporterà il rigetto della comunicazione; pertanto, si raccomanda di non aprire il file ricevuto ma esclusivamente di procedere alla sua sottoscrizione digitale, previo salvataggio in locale.

L'eventuale rigetto della comunicazione, e la relativa motivazione, saranno comunicati esclusivamente al soggetto che effettua la comunicazione, mediante l'invio di una e-mail all'indirizzo indicato nella sezione A del modulo.

Nel caso in cui la comunicazione venga accolta:

- il soggetto che effettua la comunicazione riceverà, mediante comunicazione inviata all'indirizzo email indicato nella sezione A del modulo, l'indicazione del numero di protocollo utilizzato per la registrazione dei dati comunicati; - il soggetto Titolare/Responsabile riceverà, mediante comunicazione inviata all'indirizzo PEC indicato nella sezione B (o all'altro riferimento e-mail, qualora trattasi di soggetto privo di PEC), un documento informatico contenente le informazioni inserite all'atto della compilazione del modulo e l'indicazione del numero di protocollo utilizzato per la registrazione dei dati comunicati - il soggetto designato quale RPD riceverà, mediante comunicazione inviata all'indirizzo PEC indicato al punto 5 della sezione C, un documento informatico contenente le informazioni inserite all'atto della compilazione del modulo e l'indicazione del numero di protocollo utilizzato per la registrazione dei dati

comunicati.

Per eventuali future comunicazioni con l'Autorità è necessario far riferimento al numero di protocollo e non all'identificativo provvisorio della comunicazione.

Eventuali ulteriori comunicazioni successive effettuate per conto dello stesso Titolare/Responsabile, qualora accettate, saranno intese come integrale sostituzione di quanto già comunicato in precedenza.

3. Considerazioni conclusive

Il *privacy officer* (in inglese, "agente della privacy") è una figura professionale con competenze giuridiche, informatiche e gestionali, la cui responsabilità principale è osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda, affinché questi siano trattatati in modo lecito e pertinente, nel rispetto delle normative vigenti.

Quando il soggetto che ricopre questo ruolo opera con autonomia e gli è conferito potere decisionale nello svolgimento delle proprie mansioni, si parla di *chief privacy officer (*CPO), figura che in Europa ha assunto anche la denominazione di *data protection officer* (DPO), o Responsabile della Protezione dei Dati (RPD), come reso nella versione italiana del Regolamento UE 2016/679.

Come chiarito, il DPO deve possedere un'adeguata conoscenza della normativa che regolamenta la gestione dei dati personali nel paese in cui opera. Deve dunque poter offrire ai vertici aziendali la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, curando l'adozione di un complesso di misure di sicurezza finalizzate alla tutela dei dati che soddisfino i requisiti di legge e assicurino sicurezza e riservatezza.

La protezione dei dati personali è, e deve rimanere, un tema di cruciale importanza per i vari soggetti giuridici. La capacità di assicurare la riservatezza e la sicurezza dei dati, inclusi i dati personali, rappresenta un fattore critico di successo, oltre a consentire di evitare la applicazione di sanzioni destinate a divenire ancora più pesanti con l'applicazione della normativa europea in materia di privacy.

Allegato A

Schema di atto di designazione del Responsabile della Protezione dei Dati (RPD) ai sensi dell'art. 37 del Regolamento UE 2016/679

Premesso che:

- Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *«relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»* (di seguito *RGPD*), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018, introduce la figura del Responsabile della protezione dei dati (si seguito, RPD) (artt. 37-39);
- Il predetto Regolamento prevede l'obbligo per il titolare o il responsabile del trattamento di designare il *RPD «quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali»* (art. 37, paragrafo 1, lett a);
- Le predette disposizioni prevedono che il RPD *«può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi»* (art. 37, paragrafo 6) e deve essere individuato *«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'art. 39»* (art. 37, paragrafo 5) *e «il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento»* (considerando n. 97 del RGPD);*«un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione»* (art. 37, paragrafo 3);

Considerato che *l'Ente X:*

- è tenuto alla designazione obbligatoria del RPD nei termini previsti, rientrando nella fattispecie prevista dall'art. 37, par. 1, lett a) del RGPD;

Nel caso in cui di designazione di un RPD condiviso:

- ha ritenuto di avvalersi della facoltà, prevista dall'art. 37, paragrafo 3, del Regolamento, di procedere alla nomina condivisa di uno stesso RPD con gli *Enti X, Y, Z,* sulla base delle valutazioni condotte di concerto con i predetti Enti in ordine a … (es. dimensioni, affinità tra le relative strutture organizzative, funzioni (attività) e trattamenti di dati personali, razionalizzazione della spesa);

- all'esito di … (*indicare la procedura selettiva interna o esterna, gara, altro*) ha ritenuto che (*persona fisica/persona giuridica individuata*) abbia un livello di conoscenza specialistica e delle competenze richieste dall'art. 37, par. 5, del RGPD, per la nomina a RPD, e non si trovi in situazioni di conflitto di interesse con la posizione da ricoprire e i compiti e le funzioni da espletare;

DESIGNA

(*persona fisica/persona giuridica individuata*), Responsabile della protezione dei dati (RPD) per l'*Ente X,*

Nel caso in cui si opti per la designazione di una persona giuridica, aggiungere:
il cui referente individuato per l'Ente è il Sig./Dott. *(generalità persona fisica)*;

Il RPD, nel rispetto di quanto previsto dall'art. 39, par. 1, del RGPD è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

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 RGPD, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
b) sorvegliare l'osservanza del RGPD, di altre disposizioni nazionali o dell'Unione 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'art. 35 del RGPD;
d) cooperare con il Garante per la protezione dei dati personali;
e) fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

(*è possibile inserire di seguito anche ulteriori compiti, purché non incompatibili, quali ad es.:*

f) *tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile ed attenendosi alle istruzioni impartite…)*

I compiti del Responsabile della Protezione dei Dati attengono all'insieme dei trattamenti di dati effettuati dall' Ente X.

L'*Ente X* si impegna a:

a) mettere a disposizione del RPD le seguenti risorse al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate … (*specificare, ad es. se è stato istituito un apposito Ufficio o gruppo di lavoro, le relative dotazioni logistiche e di risorse umane, nonché i compiti o le responsabilità individuali del personale*);
b) non rimuovere o penalizzare il RPD in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni;
c) garantire che il RPD eserciti le proprie funzioni in autonomia e indipendenza e in particolare, non assegnando allo stesso attività o compiti che risultino in contrasto o conflitto di interesse;

DELIBERA

di designare …… come Responsabile della Protezione dei Dati (RPD) per *l'Ente X*

Data ……..

Il nominativo e i dati di contatto del RPD (recapito postale, telefono, email) saranno resi disponibili nella intranet dell'Ente (url…., ovvero bacheca) e comunicati al Garante per la protezione dei dati personali. I dati di contatto saranno, altresì, pubblicati sul sito internet istituzionale.

Allegato B

LETTERA D'INCARICO PROFESSIONALE PER LO SVOLGIMENTO DELL'INCARICO DI D.P.O. (Data Protection Officer)
ART. 37 REG. UE 2016/679

La società (nome società) con sede in _____, Codice Fiscale _____, iscritta al Registro delle Imprese di _____ col numero _____, *conferisce incarico* al professionista _____, con studio in _____ (di seguito denominato DPO) o alla società _____ (di seguito denominato DPO), per lo svolgimento delle funzioni di Data Protection Officer (responsabile della protezione dei dati), così come previsto dall'art 37 del Reg. UE 2016/679.

Funzioni del DPO

Come indicato nell'art. 39 Reg. Ue 2016/679 il DPO dovrà:

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 regolamento 2016/679 nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

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'art. 35

d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Modalità di svolgimento dell'incarico professionale

Il DPO, per l'espletamento dell'incarico, potrà utilizzare un team di tecnici e professionisti in possesso delle professionalità necessarie per lo svolgimento delle funzioni oggetto del presente incarico i quali potranno operare anche disgiuntamente con riferimento alle fasi di svolgimento dei servizi consulenza ed assistenza.

Le attività oggetto dell'incarico saranno svolte:

- con accessi presso la società per analisi, verifiche documentali, colloqui con il management e interviste alle varie funzioni aziendali in base alle esigenze riscontrate;
- presso la sede del DPO per ricerche giuridiche e tecniche, studio di atti ed esame dei documenti, ricerche di giurisprudenza.

Gli accessi e gli incontri presso la sede della società saranno fissati secondo un calendario concordato tra le parti.
La società si obbliga:

- ad assicurare la necessaria collaborazione dei soggetti facenti parte dell'organizzazione in tutte le fasi di svolgimento dell'attività oggetto dell'incarico;
- ad assicurare la messa a disposizione di tutta la documentazione necessaria per lo svolgimento delle attività oggetto dell'incarico;

Durata dell'incarico

Il presente incarico deve intendersi valido fino al __ / __ / _____.

Risoluzione dell' incarico

Il Committente potrà procedere in qualsiasi momento alla revoca dell'incarico conferito mediante comunicazione da inviare con lettera raccomandata A/R, con pagamento del corrispettivo in base allo stato di avanzamento del lavoro.
Anche il DPO potrà recedere dal contratto dandone comunicazione mediante lettera raccomandata A/R, in tal caso il committente non sarà tenuto al pagamento del lavoro svolto fino a quel momento.

Determinazione del compenso

Il compenso complessivo spettante per l'espletamento delle prestazioni stabilite nel presente incarico ammonta a € _____ oltre IVA.

Modalità di pagamento

Il pagamento del corrispettivo stabilito avverrà in seguito all'emissione di fattura da parte del DPO secondo i seguenti importi e tempistiche:

- versamento di acconto di € _____, oltre IVA, all'atto dell'accettazione dell'incarico da parte del DPO;
- versamento di € _____, oltre IVA, con cadenza mensile per tutta la durata dell'incarico;

Utilizzo di professionisti, consulenti ed esperti esterni al DPO

Qualora il DPO riscontrasse la necessita, nell'interesse della società Committente, per il corretto espletamento dell'incarico, di affrontare particolari problematiche che esulano dall'oggetto del presente incarico, per la risoluzione delle quali si dovesse rendere necessario l'intervento di un consulente od un esperto esterni al gruppo di lavoro indicato, il DPO segnalerà l'esigenza affinchè la società Committente assuma le proprie decisioni in merito.
La segnalazione di tale necessita esonererà il Consulente da qualsiasi responsabilità in relazione allo specifico problema segnalato.

Tutela della segretezza

Tutti i dati, le informazioni e i documenti esaminati e gestiti dal DPO e dalla sua organizzazione nello svolgimento dell'incarico professionale devono essere considerati riservati. Pertanto e fatto assoluto divieto di divulgazione o comunicazione.

Privacy

In conformità a quanto disposto dal d.lgs. 196/2003, il Consulente dovrà garantire la massima riservatezza nel trattamento dei dati forniti dalla società Committente che saranno utilizzati esclusivamente per lo svolgimento dell'incarico professionale.

Il titolare della gestione dei dati sarà il Consulente _____

Luogo e data

APPENDICE

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del
27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei
dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
(regolamento generale sulla protezione dei dati)

Linea Guida in materia di responsabili della protezione dei dati (DPO)
13 dicembre 2016
La presente costituisce una traduzione non ufficiale e di cortesia in lingua italiana della versione in lingua inglese del documento 16/EN WG243: Linea Guida in materia di responsabili della protezione dei dati (DPO) 13 dicembre 2016 del WG 29 Tale traduzione (versione n.1) è stata effettuata, nell'ottica di condivisione della conoscenza, al fine di agevolare la lettura da parte di cittadini, imprese e associazioni nell'attesa della traduzione ufficiale da parte degli organi competenti. Non si assume alcuna responsabilità in merito alla correttezza della traduzione stessa.

IL GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995,visti gli articoli 29 e 30, visto il suo regolamento, ha adottato gli orientamenti presenti:

Indice dei contenuti

1. Introduzione

Il Regolamento Generale sulla Protezione dei Dati (GDPR – General Data Protection Regulation)[28], che entrerà in vigore il 25 maggio 2018, fornirà un moderno quadro basato sulla responsabilità, relativo alla conformità per la protezione dei dati in Europa. I responsabili della protezione dei dati (DPO – Data Protection Officer) saranno, per molte organizzazioni, al centro di questo nuovo quadro giuridico, facilitando così il rispetto delle disposizioni del GDPR.

Per il GDPR, è obbligatorio per alcuni titolari e responsabili, designare un DPO[29]. Questo è il caso di tutte le autorità pubbliche e gli organismi (indipendentemente da quali dati elaborino), e per altre organizzazioni che - come attività principale – hanno il monitoraggio sistematico e su larga scala delle persone, o trattano particolari categorie di dati personali su larga scala.

Anche quando il GDPR non prevede esplicitamente la nomina di un DPO, le organizzazioni possono trovare utile designare, su base volontaria, un DPO. Il Gruppo di Lavoro sulla Protezione dei Dati Articolo 29 (WP29) incoraggia tali designazioni volontarie. Il concetto di DPO non è nuovo. Anche se la direttiva 95/46 / CE[30] non obbligava nessuna organizzazione a nominare un DPO, nella pratica, la nomina del DPO si è sviluppata nel corso degli anni in vari Stati membri.

Prima dell'adozione del GDPR, il WP29 ha sostenuto che il DPO è un elemento fondamentale di responsabilità e che la nomina di un DPO possa facilitare la conformità e, inoltre, diventare un vantaggio competitivo per il business[31]. Oltre a

---

[28] Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e che abroga la direttiva 95/46 / CE (regolamento sulla protezione dei dati generali), (GU L 119, 2016/05/04).

[29] La nomina di un DPO è obbligatoria anche per le autorità competenti ai sensi dell'art. 32 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali dalle autorità competenti ai fini della prevenzione, ricerca, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, e che abroga la decisione quadro 2008/977 / GAI del Consiglio (GU L 119, 4.5. 2016, p. 89-131), e la legislazione nazionale di attuazione. Mentre queste linee guida si concentrano sul DPO del GDPR, la guida è rilevante anche per quanto riguarda il DPO ai sensi della direttiva 2016/680, per quanto riguarda le loro analoghe disposizioni.

[30] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag . 31).

[31] Vedi http://ec.europa.eu/justice/data-protection/article-29/documentation/otherdocument/files/2015/20150617_appendix_core_issues_plenary_en.pdf.

facilitare la conformità attraverso la realizzazione di strumenti di evidenza delle responsabilità (*accountability*) (ad esempio facilitare o effettuare valutazioni di impatto sulla protezione dei dati e audit), i DPO fungono da intermediari tra le parti interessate (ad esempio le autorità di vigilanza, le persone interessate e le unità di business all'interno di un'organizzazione).
Il DPO non è personalmente responsabile in caso di mancato rispetto del GDPR. Il GDPR esplicita chiaramente che sono il titolare o il responsabile tenuti a garantire ed essere in grado di dimostrare che il trattamento viene eseguito in conformità con le sue disposizioni (art. 24 (1)). Il rispetto della protezione dei dati è una responsabilità del titolare o del responsabile.
Il titolare o il responsabile hanno anche un ruolo cruciale nel consentire un efficace svolgimento dei compiti del DPO. La nomina di un DPO è un primo passo, ma il DPO deve avere sufficiente autonomia e risorse per svolgere i propri compiti in modo efficace.
Il GDPR riconosce il DPO come un attore chiave nel nuovo sistema di *governance* dei dati e stabilisce le condizioni per la sua nomina, la posizione e le attività. Lo scopo di queste linee guida è quello di chiarire le disposizioni pertinenti nel GDPR al fine di aiutare i titolari e responsabili al rispetto legislativo, ma anche di assistere il DPO nel proprio ruolo. Le linee guida forniscono anche raccomandazioni sulle *best practises*, sulla base dell'esperienza acquisita in alcuni Stati membri dell'UE. Il WP29 monitorerà l'attuazione di queste linee guida e potrà integrarle, se necessario, con ulteriori dettagli.

2. Designazione di un DPO

2.1. Designazione obbligatoria

L'art. 37 (1) del GDPR richiede la designazione di un DPO in tre casi specifici[32]:
a) quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico[33];
b) se le attività principali del titolare o del responsabile consistono in trattamenti, che richiedono un monitoraggio regolare e sistematico, su larga scala, degli interessati; o
c) quando le attività principali del titolare o il responsabile consistono in trattamenti su larga scala di categorie particolari di dati[34] o[35] dati personali in materia di condanne penali e reati[36].
Nelle seguenti sezioni, il WP29 fornisce una guida per quanto riguarda i criteri e la terminologia utilizzate all'art. 37(1).

---

[32] Si noti che ai sensi dell'art. 37 (4), l'Unione o una legge dello Stato membro possono chiedere la designazione dei DPO in altre situazioni.
[33] Fatta eccezione per i tribunali che agiscono a titolo giudiziario.
[34] Ai sensi dell'art. 9 questi includono dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici al fine di identificare in modo univoco una persona fisica, dati relativi alla salute o dati riguardanti la vita sessuale di una persona fisica o l'orientamento sessuale.
[35] Art. 37 (1) (c) usa la parola 'e'. Vedere la sezione 2.1.5, di seguito, per la spiegazione sull'uso del 'o' invece di 'e'.
[36] Art. 10.

A meno della ovvietà che l'organizzazione non sia tenuta a designare un DPO, il WP29 raccomanda che i titolari ed i responsabili documentino l'analisi interna effettuata per determinare se è necessario o meno nominare un DPO, in modo da essere in grado di dimostrare che il fattori più importanti sono stati correttamente presi in considerazione[37].
Quando un'organizzazione designa una DPO su base volontaria, gli stessi requisiti di cui agli articoli da 37 a 39 si applicano alla sua nomina, alla posizione e alle attività come se la nomina fosse obbligatoria.
Ciò non impedisce ad un'organizzazione, che non vuole designare un DPO su base volontaria e non è legalmente tenuta a designare un DPO, di utilizzare comunque consulenti esperti, con compiti relativi alla protezione dei dati personali, interni od esterni.
In questo caso è importante assicurare che non ci sia confusione riguardo il titolo, lo stato, la posizione e compiti. Pertanto, deve essere chiaro, in qualsiasi comunicazione all'interno ed all'esterno dell'azienda, così come con le autorità di protezione dei dati, con le persone interessate, e con il pubblico in generale, che il titolo di questa figura o consulente non è un DPO[38].

2.1.1. Autorità o organismo pubblico

Il GDPR non definisce cosa costituisca "un'autorità pubblica o un organismo pubblico". Il WP29 ritiene che tale nozione debba essere determinata in base al diritto nazionale. Di conseguenza, le autorità pubbliche e gli organismi comprendono le autorità nazionali, regionali e locali, ma il concetto, ai sensi delle leggi nazionali applicabili, di solito include anche una serie di altri organismi di diritto pubblico[39]. In tali casi, la designazione di un DPO è obbligatoria.
Un'attività pubblica può essere effettuata, e la pubblica autorità esercitata[40] non soltanto da autorità o enti pubblici, ma anche da altre persone fisiche o giuridiche di diritto pubblico o privato, in settori quali, secondo la normativa nazionale di ciascuno Stato membro, servizi di trasporto pubblico, fornitura di acqua ed energia, infrastrutture stradali, servizio pubblico di radiodiffusione, edilizia residenziale pubblica o organi disciplinari per le professioni regolamentate.
In questi casi, le persone interessate possono trovarsi in una situazione molto simile a quella in cui i propri dati vengono trattati da un'autorità pubblica o da un organismo. In particolare, i dati possono essere trattati per scopi simili e gli individui hanno spesso poca o nessuna scelta, su se e come i loro dati saranno trattati, e pertanto possono richiedere la protezione aggiuntiva che la nomina di un

---

[37] Si veda l'art. 24(1).

[38] Questo è importante anche per i *chief privacy officer* (CPO) o altri professionisti privacy già attivi oggi in alcune aziende, che non possono sempre soddisfare i criteri del GDPR, per esempio, in termini di disponibilità di risorse o garanzie per l'indipendenza e quindi non possono essere considerati e indicati come DPO.

[39] Si veda, ad esempio, la definizione di organismo del settore pubblico e organismo di diritto pubblico di cui all'art. 2 (1) e (2), della direttiva 2003/98 / CE del Parlamento europeo e del Consiglio del 17 novembre 2003, relativa al riutilizzo delle informazioni del settore pubblico (GU L 345 del 31.12.2003, pag. 90).

[40] Art. 6 (1) (e).

DPO può garantire.
Anche se non vi è alcun obbligo in questi casi, il WP29 raccomanda, come buona pratica,che:
• organizzazioni private incaricate di fornire servizi o esercitare l'autorità pubblica designino un DPO e che
• tale attività di DPO dovrebbe coprire tutti i trattamenti effettuati, compresi quelli che non sono legati all'esecuzione di un compito pubblico o esercizio del dovere ufficiale (ad esempio, la gestione di un database dei dipendenti).

2.1.2. Attività principali

L'art. 37 (1) (b) e (c) del GDPR si riferisce alle attività principali del titolare o del responsabile. Il considerando 97 specifica che le attività principali di un titolare si riferiscono ad "attività primarie e non si riferiscono al trattamento dei dati personali come attività accessorie". Le attività principali possono essere quindi considerate come le operazioni chiave necessarie per raggiungere gli obiettivi del titolare o del responsabile.
Tuttavia, le attività fondamentali non devono essere interpretate come escludenti le attività in cui il trattamento dei dati costituisce una parte inscindibile di attività del titolare o del responsabile. Ad esempio, l'attività principale di un ospedale è di fornire assistenza sanitaria. Tuttavia, un ospedale non ha può fornire l'assistenza sanitaria in modo sicuro ed efficace senza il trattamento dei dati relativi alla salute, come ad esempio le cartelle cliniche dei pazienti. Pertanto, il trattamento di questi dati deve essere considerato come una delle attività principali di ogni ospedale, pertanto questi, devono designare il DPO. Un altro esempio potrebbe essere quello di una società di sicurezza privata che svolge la sorveglianza di un certo numero di centri commerciali privati e spazi pubblici. La sorveglianza è l'attività principale della società, che a sua volta è indissolubilmente legata al trattamento dei dati personali. Pertanto, questa società deve designare un DPO.
D'altra parte, tutte le organizzazioni svolgono diverse attività, ad esempio, pagano i loro dipendenti o hanno attività standard IT. Si tratta di funzioni di supporto necessarie per svolgere l'attività principale dell'organizzazione o per raggiungere il business. Anche se queste attività sono necessarie o essenziali, di solito sono considerate funzioni accessorie, rispetto all'attività principale.

2.1.3. Larga scala

Art. 37 (1) (b) e (c), richiede la nomina del DPO per il trattamento dei dati personali effettuato su larga scala. Il GDPR non fornisce una definizione di larga scala, anche se il considerando 91 illustra alcune indicazioni[41].

[41] Secondo il considerando, 'le operazioni di trattamento su larga scala che mirano a elaborare una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che possano interessare un gran numero di persone interessate e che sono suscettibili di causare un alto rischio' dovrebbero essere incluse. D'altra parte, il considerando prevede espressamente che il trattamento dei dati personali non dovrebbe essere considerato su larga scala se il trattamento riguarda dati personali provenienti da pazienti o clienti da parte di un singolo medico, o altro operatore sanitario o avvocato. È importante considerare che, mentre il considerando fornisce esempi agli estremi della scala (elaborazione da parte di un singolo medico contro trattamento di dati di un intero paese o in Europa), c'è una grande zona grigia tra questi due estremi. Inoltre, va tenuto presente che questo considerando fa riferimento alle valutazioni d'impatto sulla protezione dei dati. Ciò

Infatti, non è possibile dare un numero preciso sia per quanto riguarda la quantità di dati elaborati o il numero di persone interessate, che sia applicabile a tutte le situazioni. Ciò non esclude la possibilità, tuttavia, che nel corso del tempo, possa svilupparsi una pratica standard, per specificare in termini oggettivi e quantitativi ciò che costituisce il trattamento su larga scala di alcuni tipi di attività comuni. Il WP29 prevede inoltre al contributo, attraverso la condivisione e la pubblicazione di esempi di soglie rilevanti per la designazione di un DPO, a questo sviluppo. In ogni caso, il WP29 raccomanda che, in particolare, i seguenti fattori devono essere presi in considerazione per determinare se il trattamento è effettuato o meno su larga scala:

• Il numero di persone interessate - sia come un numero specifico o come percentuale della popolazione in questione
• Il volume di dati e / o la gamma di differenti elementi di dati in elaborazione
• La durata, o la permanenza, l'attività di elaborazione dei dati
• L'estensione geografica dell'attività del trattamento

Esempi di trattamenti su larga scala includono:

• l'elaborazione dei dati del paziente nel corso normale delle attività di un ospedale
• trattamento dei dati di viaggio di persone che utilizzano il sistema di trasporto pubblico di una città (ad esempio, il monitoraggio tramite schede di viaggio)
• l'elaborazione dei dati in tempo reale di geo-localizzazione di clienti di una catena di fast food internazionale a fini statistici da parte di un responsabile specializzato nella fornitura di questi servizi
• trattamento dei dati dei clienti nel normale corso di attività da una compagnia di assicurazioni o di una banca
• trattamento dei dati personali (profilazione) per la pubblicità di un motore di ricerca
• trattamento dei dati (contenuti, il traffico, la posizione) da parte dei fornitori di servizi telefonici o Internet

Esempi che non costituiscono l'elaborazione su larga scala sono:

• trattamento dei dati dei pazienti da parte di un singolo medico
• trattamento di dati personali relativi a condanne penali e reati da parte di un singolo avvocato.

2.1.4. Monitoraggio regolare e sistematico

La nozione di un monitoraggio regolare e sistematico degli interessati, non è definito nel GDPR, ma il concetto di monitorare il comportamento degli interessati è menzionato nel considerando 24[42] e comprende in modo chiaro tutte le forme di monitoraggio e profilatura su internet, anche per i fini della pubblicità

---

implica che alcuni elementi potrebbero essere specifici per quel contesto e non necessariamente si applicano alla designazione dei DPO esattamente allo stesso modo.

[42]Al fine di determinare se un'attività può essere considerata di monitoraggi del comportamento degli interessati, occorre verificare se le persone fisiche sono tracciate su Internet compreso il potenziale utilizzo successivo di tecniche di elaborazione dei dati personali che consistono nel profilare una persona fisica, in particolare al fine di prendere decisioni in materia di lei o di lui o per l'analisi e la previsione di lei o di lui delle sue preferenze personali, comportamenti e atteggiamenti.

comportamentale.
Tuttavia, il concetto di monitoraggio deve essere considerato soltanto come un esempio di monitoraggio del comportamento degli interessati[43]. WP29 interpreta come definizione di "regolare" il verificarsi di uno o più dei seguenti
elementi:
• in corso o che si verificano a intervalli specifici per un determinato periodo
• ricorrente o ripetuto ad orari prestabiliti
• costantemente o periodicamente svolto
WP29 interpreta la definizione di "sistematico" il verificarsi di uno o più dei seguenti elementi:
• il verificarsi in base ad un sistema
• pre-organizzato, organizzato o metodico
• che si svolge nell'ambito di un piano generale per la raccolta dati
• eseguito come parte di una strategia
Esempi:
operatori di una rete di telecomunicazioni; fornitura di servizi di telecomunicazione; e-mail retargeting; profilazione e scoring ai fini della valutazione del rischio (ad esempio a scopo di recupero crediti, istituzione di premi assicurativi, la prevenzione delle frodi, l'individuazione di riciclaggio di denaro); tracciabilità della posizione, programmi di fidelizzazione; pubblicità legata ai comportamenti (profilazione); monitoraggio di benessere, fitness e salute dati tramite dispositivi indossabili; televisione a circuito chiuso; dispositivi collegati a contatori intelligenti, macchine intelligenti, domotica, ecc.

2.1.5. Categorie particolari di dati e dati relativi a condanne penali e reati

L'art. 37 (1) (c) affronta il trattamento di categorie particolari di dati ai sensi dell'art. 9, e dati personali relativi a condanne penali e reati di cui all'art. 10. Anche se la dicitura usa la parola 'e', non vi è alcuna ragione per cui i due criteri debbano essere applicati contemporaneamente. Il testo dovrebbe quindi essere letto come 'o'.

2.2. DPO del responsabile

L'art. 37 si applica sia ai titolari[44] che ai responsabili[45] per quanto riguarda la designazione di un DPO. A seconda di chi soddisfa i criteri sulla designazione obbligatoria, cioè in alcuni casi solo il titolare o solo il responsabile, oppure in altri casi, sia il titolare e il responsabile sono tenuti a nominare un DPO (che dovrebbero quindi cooperare tra loro).
È importante sottolineare che anche se il titolare soddisfa i criteri per la

[43] Si noti che il considerando 24 si concentra sulla applicazione extraterritoriale del GDPR. Inoltre, vi è anche una differenza tra la dicitura "monitorare il loro comportamento" (art. 3 (2) (b)), e "monitoraggio regolare e sistematico delle persone interessate" (art. 37 (1) (b)), che potrebbe quindi essere visto come parte di una diversa nozione.
[44] Il titolare è definito dall'art. 4 (7) come la persona fisica o giuridica, che determina le finalità e gli strumenti del trattamento.
[45] Il responsabile è definito dall'art. 4 (8) come la persona fisica o giuridica, che elabora i dati per conto del titolare.

designazione obbligatoria, il suo responsabile non è necessariamente tenuto a nominare un DPO. Questo può, tuttavia, però essere una buona prassi.
Esempi:
• Una piccola azienda familiare attiva nella distribuzione di elettrodomestici in un unico comune, utilizza i servizi di un responsabile la cui attività principale consiste nel fornire servizi di analisi di siti web e di assistenza con pubblicità mirata e marketing. Le attività dell'azienda di famiglia e dei suoi clienti non generano l'elaborazione di dati su larga scala, considerando il piccolo numero di clienti e le attività relativamente limitate. Tuttavia, le attività del responsabile (una PMI), che possiede in tal modo molti clienti, presi insieme, possono configurarsi come trattamenti su larga scala. Il responsabile deve quindi nominare un DPO ai sensi dell'art. 37 (1) (b). Allo stesso tempo, l'azienda di famiglia in sé non ha l'obbligo di designare un DPO.
• una società di produzione di piastrelle di medie dimensioni subappalta i servizi di medicina del lavoro ad un responsabile esterno, che possiede un gran numero di clienti simili. Il responsabile designa un DPO ai sensi dell'art. 37 (1) (c) a condizione che il trattamento sia su larga scala. Tuttavia, il produttore non è necessariamente obbligato a nominare un DPO.
Come buona prassi, il WP29 raccomanda che il DPO, designato da un responsabile, dovrebbe anche supervisionare le attività svolte dall'organizzazione in qualità di titolari del trattamento vero e proprio (ad esempio risorse umane, IT, logistica).

2.3. Facilmente raggiungibile da ogni stabilimento

Art. 37 (2) permette ad un gruppo di imprese di designare un unico DPO a condizione che questi sia facilmente raggiungibile da ogni stabilimento. Il concetto di accessibilità si riferisce ai compiti del DPO come un punto di contatto rispetto agli interessati[46], all'autorità di controllo[47] ma anche internamente all'organizzazione, considerando che uno dei compiti del DPO è informare e consigliare, dei loro obblighi ai sensi della presente Regolamento[48], il titolare, il responsabile e i dipendenti che svolgono trattamenti. Al fine di garantire che il DPO, interno o esterno, sia accessibile e contattabile è importante garantire che il suo indirizzo di contatto sia disponibile in conformità con i requisiti del GDPR[49].
Il DPO deve essere in grado di comunicare in modo efficiente con gli interessati[50]

---

[46] L'art. 38 (4): gli interessati possono contattare il responsabile della protezione dei dati per quanto riguarda tutte le questioni relative al trattamento dei propri dati personali e per l'esercizio dei loro diritti ai sensi del presente regolamento.

[47] L'art. 39 (1) (e): 'fungere da punto di contatto per l'autorità di controllo su questioni relative al trattamento, tra cui la consultazione preliminare di cui all'art. 36, e di consultare, se del caso, in relazione a qualsiasi altra questione'.

[48] L'art. 39 (1) (a).

[49] Vedi anche la sezione 2.5.

[50] L'art. 12 (1): Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'art. 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

e cooperare[51] con le autorità di vigilanza. Questo significa anche che tale comunicazione deve avvenire nella lingua o nelle lingue utilizzate dalle autorità di controllo e delle persone interessate. Ai sensi dell'art. 37 (3), un singolo DPO può essere designato per più autorità o enti pubblici, tenendo conto della loro struttura e dimensione organizzativa. Le stesse considerazioni valgono per quanto riguarda le risorse e la comunicazione. Dato che il DPO è responsabile di una serie di compiti, il titolare deve garantire che un singolo DPO sia in grado di eseguire in modo efficiente ed efficace questi compiti, pur essendo responsabile di diversi enti pubblici ed enti. La disponibilità personale di un DPO (sia fisicamente negli stessi locali come dipendenti, attraverso un numero verde o altro mezzo di comunicazione sicuro) è essenziale per garantire che gli interessati siano in grado di contattare il DPO. Il DPO è tenuto al segreto o alla riservatezza relativa al rendimento dei suoi compiti, in conformità con il diritto dell'Unione o Stato membro (art. 38 (5)). Tuttavia, l'obbligo del segreto / riservatezza non vieta il che il DPO possa contattare e chiedere un parere all'autorità di vigilanza.

2.4. Competenze e capacità del DPO

Art. 37 (5), prevede che il DPO 'è designato in base alla qualità professionali e, in particolare, conoscenza approfondita del diritto alla protezione dei dati, delle pratiche e la capacità di svolgere i compiti di cui all'art. 39'. Il considerando 97 prevede che il livello necessario di conoscenze specialistiche deve essere determinato in base ai trattamenti dei dati effettuati e la loro protezione.

• **Livello di esperienza**

Il livello richiesto di competenza non è strettamente definito ma deve essere commisurato con la sensibilità, la complessità e la quantità di dati dei processi organizzativi. Ad esempio, quando un trattamento è particolarmente complesso, o se comporta una grande quantità di dati sensibili, per il DPO potrebbe essere necessario un più elevato livello di competenza e di supporto. C'è anche una differenza a seconda che l'organizzazione trasferisca sistematicamente dati personali al di fuori dell'Unione Europea o se tali trasferimenti siano occasionali. Il DPO dovrebbe quindi essere scelto con cura, tenendo conto delle questioni relative alla protezione dei dati che sorgono all'interno dell'organizzazione.

• **Qualità professionali**

Anche se l'art. 37 (5) non specifica le qualità professionali che devono essere considerate quando si designa un DPO, è importate il fatto che il DPO debba avere esperienza sulla legislazione relativa alla protezione dei dati personali sia nazionale che europea, sulle prassi e debba avere una conoscenza approfondita del GDPR. Risulta utile che le autorità di controllo promuovano una formazione adeguata e regolare per i DPO. Risulta utile la conoscenza del settore di business delle imprese e dell'organizzazione del titolare. Il DPO dovrebbe anche avere una conoscenza sui processi di trattamento dei dati e sulle operazioni effettuate, nonché sui sistemi informativi, le esigenze di sicurezza dei dati e la protezione dei dati del titolare. Nel caso di un ente pubblico o di un organismo, il DPO dovrebbe anche avere una buona conoscenza delle regole e delle procedure amministrative

[51] L'art. 39 (1) (d): a cooperare con l'autorità di controllo.

dell'organizzazione.

• Capacità di svolgere i suoi compiti

La capacità di soddisfare i compiti del DPO deve essere interpretata sia in riferimento alle sue qualità personali e alla conoscenza, ma anche in riferimento alla sua posizione all'interno dell'organizzazione. Le qualità personali dovrebbero includere, per esempio: integrità e alta etica professionale; la preoccupazione primaria del DPO dovrebbe essere di garantire la conformità al GDPR. Il DPO svolge un ruolo chiave nella promozione di una cultura della protezione dei dati all'interno dell'organizzazione e aiuta ad implementare gli elementi essenziali del GDPR, come ad esempio i principi di trattamento dei dati[52], diritti degli interessati[53], la protezione dei dati fin dalla progettazione e per default[54], la registrazione delle attività[55], la sicurezza dei trattamenti[56], la notifica e la comunicazione dei dati breach[57].

• DPO sulla base di un contratto di servizio

La funzione del DPO può essere esercitata anche sulla base di un contratto di servizio stipulato con una persona o un'organizzazione esterna all'organizzazione del titolare / responsabile. In quest'ultimo caso, è essenziale che ogni membro dell'organizzazione che esercita le funzioni di DPO soddisfi tutti i requisiti relativi alla sezione 4 della GDPR (ad esempio, è essenziale che nessuno abbia un conflitto di interessi). E' altrettanto importante che ogni membro sia protetto dalle disposizioni del GDPR (ad esempio senza la cessazione abusiva di contratto di servizio per attività come DPO, ma anche nessun licenziamento senza giusta causa di un singolo membro dell'organizzazione durante lo svolgimento dei compiti di DPO). Allo stesso tempo, le singole abilità e capacità possono essere combinate in modo che diverse persone, che lavorano in team, possano servire più efficacemente i clienti. Per motivi di chiarezza giuridica e di buona organizzazione si raccomanda di avere una chiara ripartizione dei compiti e ruoli all'interno del team del DPO e assegnare ad una singola persona il ruolo di riferimento univoco di contatto e di responsabile per ogni cliente. Sarebbe generalmente utile anche specificare questi punti nel contratto di servizio.

2.5. Pubblicazione e comunicazione delle informazioni di contatto del DPO

L'art. 37 (7) del GDPR richiede al titolare o al responsabile:

• di pubblicare i dati di contatto del DPO e

• di comunicare i dati di contatto alle autorità di controllo competenti.

L'obiettivo di questi requisiti è quello di garantire che gli interessati (sia all'interno che all'esterno dell'organizzazione) e le autorità di controllo possono facilmente, direttamente ed in maniera riservata contattare il DPO senza dover contattare un'altra parte dell'organizzazione.

---

[52] Capitolo II.

[53] Capitolo III.

[54] Articolo 25.

[55] Articolo 30.

[56] Articolo 32.

[57] Articoli 33 e 34.

I dati di contatto del DPO dovrebbero includere informazioni che consentano alle persone interessate e alle autorità di controllo di raggiungere il DPO in modo semplice (un indirizzo postale, un numero di telefono dedicato, e un indirizzo di posta elettronica dedicato). Se necessario, ai fini della comunicazione con il pubblico, possono anche essere previsti altri mezzi di comunicazione, per esempio, un numero verde dedicato o un modulo di contatto dedicato rivolti al DPO, magari sul sito web dell'organizzazione. L'articolo 37 (7) non richiede che i dati di contatto pubblicati debbano includere il nome del DPO. Anche se includere il nome può essere una buona prassi, è il titolare e il DPO che possono decidere se ciò sia necessario, o utile in circostanze particolari[58].
Il WP29 raccomanda che l'organizzazione informi l'autorità di controllo e i dipendenti del nome e dei recapiti del DPO. Ad esempio, il nome e i recapiti del DPO potrebbero essere pubblicati internamente sulla rete Intranet dell'organizzazione, o sull'elenco telefonico interno e negli organigrammi.

3. Posizione del DPO

3.1. Il coinvolgimento del DPO in tutte le questioni relative alla protezione dei dati personali

L'articolo 38 del GDPR prevede che il titolare e il responsabile assicurino che il DPO sia coinvolto, correttamente e in modo tempestivo, in tutte le questioni che riguardano la protezione dei dati personali. E' fondamentale che il DPO sia coinvolto il prima possibile in tutte le questioni relative alla protezione dei dati. In relazione alle valutazioni di impatto sulla protezione dei dati il GDPR prevede esplicitamente il precoce coinvolgimento del DPO e specifica che il titolare deve chiedere il parere del DPO nello svolgimento di tale valutazione di impatto[59]. Risulta importante garantire che il DPO sia informato e consultato, in via preliminare, in modo da facilitare il rispetto del GDPR, inoltre garantire il rispetto di un approccio "privacy by design" attraverso una procedura standard adottata all'interno dell'organizzazione. Inoltre, è importante che il DPO possa essere visto come un interlocutore all'interno dell'organizzazione e che sia parte dei gruppi di lavoro che si occupano di attività di trattamento dei dati all'interno dell'organizzazione.
Di conseguenza, l'organizzazione deve garantire, ad esempio, che:
• il DPO sia invitato a partecipare regolarmente alle riunioni di dirigenti e quadri.
• la sua presenza è raccomandata in tutti i casi in cui vengono prese le decisioni con implicazioni sulla protezione dei dati. Tutte le informazioni pertinenti devono essere trasmesse al DPO in modo tempestivo al fine di consentirgli di fornire consulenza adeguata.
• al parere del DPO deve essere sempre dato il giusto peso. In caso di disaccordo, il WP29 raccomanda, come buona pratica, di documentare le ragioni per le quali non si ritiene opportuno seguire il consiglio del DPO.

[58] È da notare che l'articolo 33 (3) (b), che descrive le informazioni che devono essere fornite alle autorità di controllo e alle persone interessate, in caso di una violazione dei dati personali, a differenza dell'articolo 37 (7), in particolare richiede che siano comunicati anche il nome (e non solo i dati di contatto) del DPO.
[59] Articolo 35 (2).

• il DPO deve essere tempestivamente consultato nel caso di violazione dei dati o nel caso in cui si verifichi un altro tipo di incidente.
Quando necessario, il titolare o il responsabile può elaborare delle linee guida sulla protezione dei dati o dei programmi che stabiliscono quando il DPO debba essere consultato.

3.2. Risorse necessarie
L'articolo 38 (2) del GDPR richiede che l'organizzazione, per sostenere il DPO, 'fornisca le risorse necessarie per svolgere [suoi] compiti e l'accesso ai dati personali ed operazioni di trattamento, e di mantenere la sua conoscenza specialistica. In particolare, sono da considerare i seguenti elementi:
• Sostegno attivo della funzione del DPO da parte della direzione (ad esempio dall'alta Direzione).
• Tempo sufficiente per il DPO per adempiere ai suoi doveri. Ciò è particolarmente importante nel caso in cui il DPO è nominato su base part-time o quando il lavoratore svolge la protezione dei dati in aggiunta ad altri compiti. In caso contrario, dei conflitti di priorità potrebbero comportare che le funzioni del DPO vengano trascurate. Avere un tempo sufficiente da dedicare ai compiti del DPO è di primaria importanza. Si tratta di buona prassi stabilire una percentuale di tempo per la funzione di DPO dove questa non venga eseguita a tempo pieno. E' anche buona pratica determinare il tempo necessario per svolgere la funzione, il livello appropriato di priorità per le funzioni del DPO, e per il DPO (o l'organizzazione) di elaborare un piano di lavoro
• Sostegno adeguato in termini di risorse finanziarie, infrastrutture (locali, strutture, attrezzature) e del personale, se del caso.
• Comunicazione ufficiale della designazione del DPO a tutto il personale al fine di garantire che la sua esistenza e la funzione sia conosciuta all'interno dell'organizzazione.
• Necessario accesso ad altri servizi, quali le risorse umane, legale, IT, sicurezza, ecc, in modo che i DPO possano ricevere supporto essenziale, input e informazioni da questi altri servizi.
• Formazione continua. Al DPO dovrebbe essere data la possibilità di rimanere aggiornato in materia di protezione dei dati. L'obiettivo dovrebbe essere quello di aumentare costantemente il livello di competenza del DPO e dovrebbe essere incoraggiato a partecipare a corsi di formazione sulla protezione dei dati e altre forme di sviluppo professionale, come la partecipazione in privacy forum, workshop, ecc
• Date le dimensioni e la struttura dell'organizzazione, può essere necessario allestire una squadra di DPO (un DPO e il suo staff). In questi casi, la struttura interna della squadra e dei compiti e delle responsabilità di ciascuno dei suoi membri dovrebbe essere chiaramente redatta. Allo stesso modo, quando la funzione del DPO è esercitata da un fornitore esterno, un gruppo di persone, che lavorano per questa entità, possono efficacemente svolgere i compiti di un DPO come una squadra, sotto la responsabilità di un responsabile di contatto designato per il cliente.
In generale maggiori sono i trattamenti e la loro complessità o i trattamenti sensibili, maggiori devono essere le risorse allocate per il DPO. La funzione di

protezione dei dati deve essere efficace e sufficientemente costruita in relazione ai trattamenti dei dati in corso.

3.3. Istruzioni e "agire in modo indipendente"

L'articolo 38 (3) stabilisce alcune garanzie di base per contribuire a garantire che il DPO sia in grado di svolgere i suoi compiti con un sufficiente grado di autonomia all'interno dell'organizzazione. In particolare, il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il considerando 97 aggiunge che il DPO 'anche se non è un dipendente del titolare, dovrebbe essere in grado di svolgere le sue funzioni e compiti in modo indipendente '. Ciò significa che, nell'adempimento dei suoi compiti di cui all'articolo 39, il DPO non deve essere istruito su come affrontare una questione, per esempio, quale risultato dovrebbe essere raggiunto, come indagare su una denuncia o se è necessario consultare l'autorità di controllo. Inoltre i DPO, non devono ricevere indicazioni su come avere un particolare punto di vista in merito ad un problema relativo alla legge sulla protezione dei dati, per esempio, una particolare interpretazione della legge. L'autonomia dei DPO, tuttavia, non significa che essi hanno poteri decisionali che si estendono oltre i loro compiti di cui all'articolo 39.

Il titolare o il responsabile rimangono responsabili per il rispetto della normativa sulla protezione dei dati e devono essere in grado di dimostrarne la conformità[60]. Se il titolare o il responsabile prende decisioni che sono incompatibili con il GDPR e con il parere del DPO, al DPO deve essere data la possibilità di rendere chiara la propria opinione dissenziente a coloro che devono prendere le decisioni.

3.4. Licenziamento o penali per l'esecuzione di attività del DPO

L'articolo 38 (3) richiede anche che il DPO dovrebbe 'non essere licenziato o subire penali o richiami dal titolare o responsabile per l'esecuzione dei [suoi] compiti'.

Questo requisito rafforza anche l'autonomia dei DPO e aiuta a garantire che essi possano agire in modo indipendente e godere di una protezione sufficiente nello svolgimento delle loro attività di protezione dei dati.

Le sanzioni sono vietate, secondo il GDPR, solamente se sono inflitte a seguito del fatto che il DPO svolga o abbia svolto le sue funzioni come DPO. Ad esempio può succedere che un DPO consideri che un particolare trattamento è suscettibile di provocare un rischio elevato e consigliare il titolare o il responsabile di effettuare una valutazione d'impatto sulla protezione dei dati, e che il titolare o il responsabile non sia d'accordo con la valutazione del DPO. In una tale situazione, il DPO non può essere licenziato per aver fornito questo consiglio.

Le sanzioni possono assumere una varietà di forme e possono essere dirette o indirette. Esse potrebbero consistere, ad esempio, nella assenza o nel ritardo della promozione; prevenzione da avanzamento di carriera; rifiuto da benefici che altri dipendenti ricevono.

---

[60] Articolo 5 (2).

Non è necessario che tali sanzioni siano effettivamente eseguite, una semplice minaccia è sufficiente fintanto che vengono utilizzate per penalizzare il DPO per motivi legati alla sua o alle sue attività in qualità di DPO.
Come normale regola di gestione e come sarebbe il caso per qualsiasi altro dipendente o imprenditore, o soggetto a contratto nazionale applicabile o del lavoro e del diritto penale, un DPO potrebbe ancora essere licenziato legittimamente per motivi diversi a quelli legali all'esecuzione dei suoi compiti (per esempio, in caso di furto, molestie fisiche, psicologiche o sessuali o simili atti di colpa grave). In questo contesto, va notato che il GDPR non specifica come e quando un DPO può essere licenziato o sostituito da un'altra persona. Tuttavia, più stabile è il contratto di DPO, o esistono maggiori garanzie contro il licenziamento ingiusto, più è probabile che sarà in grado di agire in modo indipendente. Pertanto, il WP29 accoglierebbe con favore gli sforzi delle organizzazioni in tal senso.

3.5. Conflitto d'interessi

L'articolo 38 (6) permette al DPO di 'compiere altri compiti e mansioni'. Si richiede, tuttavia, che l'organizzazione assicuri che 'tali compiti e dei doveri non diano luogo ad un conflitto di interessi'.
L'assenza di conflitto di interessi è strettamente legata alla necessità di agire in modo indipendente. Anche se il DPO è autorizzato ad avere altre funzioni, possono essergli affidati solo altri compiti che non diano luogo a conflitti di interesse. Ciò comporta, in particolare, che il DPO non può tenere una posizione all'interno dell'organizzazione che porta a determinare le finalità e gli strumenti del trattamento di dati personali. Questo deve essere considerato caso per caso in funzione della specifica struttura organizzativa in ogni organizzazione[61].
A seconda delle attività, delle dimensioni e della struttura dell'organizzazione, può essere utile per i titolari o responsabili:
• individuare le posizioni che sarebbero incompatibili con la funzione di DPO
• elaborare il regolamento interno al fine di evitare conflitti di interesse
• includere una spiegazione più generale sui conflitti di interesse
• dichiarare che il DPO non ha alcun conflitto di interessi per quanto riguarda la sua funzione di DPO, in modo da aumentare la consapevolezza su questo requisito
• includere le garanzie, nelle regole interne dell'organizzazione, e garantire che l'avviso di posto vacante per il posto di DPO o per il contratto di servizio sia sufficientemente preciso e dettagliato, al fine di evitare un conflitto di interessi. In questo contesto, va anche tenuto presente che i conflitti di interesse possono assumere forme diverse a seconda che il DPO sia assunto internamente o esternamente.

[61]Come regola generale, le posizioni contrastanti possono includere posizioni di senior management (come amministratore delegato, direttore operativo, direttore finanziario, capo ufficiale medico, capo del dipartimento di marketing, capo delle risorse umane o capo di reparti IT), ma anche altri ruoli più in basso nella struttura organizzativa se tali posizioni o ruoli portano alla determinazione delle finalità e modalità del trattamento.

4. Compiti del DPO

4.1. Controllo del rispetto del GDPR

L'articolo 39 (1) (b) affida al DPO, tra gli altri compiti, il compito di controllare il rispetto del GDPR. Il considerando 97 specifica inoltre che il DPO 'dovrebbe aiutare il titolare o il responsabile al monitoraggio della *compliance i*nterna del rispetto del presente regolamento'.

Come parte di questi compiti per controllare la *compliance*, i DPO possono, 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 o al responsabile.

Il controllo del rispetto non significa che il DPO sia personalmente responsabile nel caso in cui vi sia una non conformità. Il GDPR rende chiaro che è il titolare, non il DPO, che è tenuto ad 'attuare misure tecniche e organizzative per garantire e per essere in grado di dimostrare che il trattamento viene eseguito in conformità del presente regolamento' (articolo 24 (1)). Il rispetto della protezione dei dati è una responsabilità aziendale del titolare del trattamento, non del DPO.

4.2. Il ruolo del DPO in una valutazione d'impatto sulla protezione dei dati

Ai sensi dell'articolo 35 (1), è compito del titolare, non del DPO, effettuare, quando necessario, una protezione dei dati di valutazione dell'impatto (DPIA-*Data Protection Impact Assessment*). Tuttavia, il DPO può svolgere un ruolo molto importante e utile per supportare il titolare. Seguendo il principio della protezione dei dati "by design", l'articolo 35 (2) richiede espressamente che il titolare 'deve chiedere il parere' del DPO nello svolgimento di un'attività di DPIA. L'articolo 39 (1) (c), a sua volta, cita tra i compiti del DPO quello di 'fornire consulenza ove richiesto per quanto riguarda il [DPIA] e monitorare le sue prestazioni'.

Il WP29 raccomanda che il titolare chieda, tra gli altri, il parere del DPO, sui seguenti temi[62]:

• effettuare o meno un DPIA
• metodologia da seguire nello svolgimento di un'attività di DPIA
• se effettuare un DPIA in-house o se esternalizzare
• quali garanzie (comprese le misure tecniche e organizzative) da applicare per mitigare gli eventuali rischi per i diritti e gli interessi delle persone interessate
• se la valutazione dei dati di impatto di protezione è stata effettuata correttamente e se le sue conclusioni e pianificazioni sono conformi al GDPR.

Se il titolare non è d'accordo con la consulenza fornita dal DPO, la documentazione del DPIA dovrebbe specificamente giustificare per iscritto il motivo per cui il consiglio non è stato preso in conto[63].

---

[62] L'articolo 39 (1) cita i compiti del DPO e indica che il DPO deve avere "almeno" i seguenti compiti. Pertanto, nulla impedisce al titolare di assegnare al DPO altri compiti diversi da quelli esplicitamente menzionati all'articolo 39 (1), o specificando i compiti in modo più dettagliato.

[63] Articolo 24 (1), prevede che 'tenuto conto della natura, la portata, il contesto e le finalità del trattamento, nonché i rischi delle variazioni della probabilità e la gravità per i diritti e le libertà delle persone fisiche, il titolare deve attuare misure tecniche ed organizzative al fine di garantire e di essere in grado di dimostrare che il trattamento viene eseguito in conformità del presente

Il WP29 raccomanda inoltre che il titolare deve delineare con chiarezza, ad esempio, nel contratto del DPO, ma anche nelle informazioni fornite ai dipendenti (e altre parti interessate, se del caso), la gestione, i compiti precisi e la loro portata del DPO, in particolare per quanto riguarda la realizzazione del DPIA.

4.3. Approccio risk-based

L'articolo 39 (2) richiede che il DPO 'deve tenere debitamente in conto del rischio associato alle operazioni di trattamento, tenuto conto della natura, la portata, il contesto e le finalità del trattamento' cioè è necessaria una valutazione corretta dei rischi. Questo articolo richiama un principio di senso più generale e comune, che può essere rilevante per il lavoro quotidiano del DPO. In sostanza, si richiede ai DPO di dare la priorità alle attività e concentrare i gli sforzi su questioni che presentino un rischio più elevato di protezione dei dati. Questo non significa che essi debbano trascurare il controllo del rispetto dei dati di operazioni che hanno un livello relativamente più basso di rischio di trattamento, ma indica che essi dovrebbero concentrarsi, in primo luogo, sulle aree a più alto rischio.
Questo approccio selettivo e pragmatico dovrebbe aiutare il DPO a consigliare al titolare quale metodologia utilizzare nello svolgimento di un DPIA, quali settori dovrebbero essere oggetto di un controllo di protezione dei dati sia interni che esterni, quali attività di formazione interna sia necessario fornire al personale o al management per le attività di trattamento dei dati.

4.4. Il ruolo del DPO nella tenuta dei registri

Ai sensi dell'articolo 30 (1) e (2), è il titolare o il responsabile, non il DPO, che è tenuto a 'mantenere un registro delle operazioni di trattamento sotto la propria responsabilità' o 'di mantenere un registro di tutte le categorie di attività di trattamento svolte per conto di un titolare'.
In pratica, i DPO spesso creano degli inventari e tengono un registro dei trattamenti sulla base delle informazioni ricevute dai vari reparti in merito al trattamento dei dati personali.
Questa pratica è stata stabilita in rispetto a molte leggi nazionali vigenti e in base alle norme sulla protezione dei dati applicabili alle istituzioni e organismi UE[64].
L'articolo 39 (1), prevede un elenco dei compiti che il DPO deve avere come minimo. Pertanto, nulla impedisce al titolare o al responsabile di assegnare al DPO il compito di mantenere il registro delle operazioni di trattamento, sotto la responsabilità del titolare.
Tale registro dovrebbe essere considerato come uno degli strumenti che permettono al DPO di svolgere i suoi compiti di controllo della conformità, informando e consigliando il titolare o il responsabile.
In ogni caso, il registro di cui è necessaria la conservazione a norma dell'articolo 30, dovrebbe essere visto come uno strumento che consenta il controllo, su richiesta da parte dell'autorità di controllo, e di avere una panoramica di tutte le attività di trattamento dei dati personali che un'organizzazione sta svolgendo. È quindi un prerequisito per la conformità, e come tale, risulta una misura di

---

regolamento. Tali misure sono riviste e aggiornate, ove necessario '
[64] Articolo 24 (1) (d), del regolamento (CE) 45/2001.

accountability.

Quarta copertina

La Commissione Privacy & Security del Consiglio dell'Ordine degli Avvocati di Napoli ha inteso dedicare un approfondimento alla figura del Data Protection Officer (DPO) istituita dal Regolamento Europeo sulla protezione dei dati personali UE 2016/679 (GDPR), essendo una delle novità più significative apportate dal Regolamento.

La nuova figura professionale si presenta con caratteristiche peculiari che ne fanno un riferimento per la corretta applicazione della normativa sia nel consesso delle Aziende private che nel settore delle Pubbliche Amministrazioni.

Con riferimento all'ambito pubblico, in particolare, il ruolo di DPO implica, di fatto, il riconoscimento ancora sottovalutato, di importanti funzioni di controllo dei procedimenti amministrativi e conseguenti responsabilità, svolte in totale autonomia ed indipendenza.