Simone Bongiovanni - Costanza Mottino - Monica Perego

IL FORMULARIO DEL DPO

Norme, giurisprudenza, strumenti operativi e modelli di atti

G. Giappichelli Editore

GUIDA ALLA LETTURA

1. I destinatari

Il testo si rivolge:

- ai Responsabili della protezione dei dati che devono mettere in atto strumenti per sorvegliare l'applicazione del Regolamento.
- ai vertici delle Organizzazioni che devono nominare un Responsabile della protezione dei dati, definire il contratto e individuare le modalità più efficaci affinché possa adempiere.
- ai vertici delle Organizzazioni che devono valutare se nominare un Responsabile della protezione dei dati e comprendere i benefici che ne possono trarre.
- ai Referenti privacy che hanno necessità di comprendere come supportare al meglio il Responsabile della protezione dei dati.
- agli auditor della privacy che cercano una metodologia consolidata, valida al di là delle evoluzioni normative a supporto del Responsabile della protezione dei dati.
- a chi svolge audit sui Sistemi di gestione della sicurezza delle informazioni e dei dati personali (es. ISO/IEC 27001:2013 ISO/IEC 27701:2019 e BS 10012:2017) e vuole ampliare il suo campo di azione.
- ai consulenti che si occupano di normativa in materia di protezione dei dati, di sicurezza delle informazioni e di Sistemi di gestione sulla protezione dei dati personali.
- a chi si occupa della stesura di clausole contrattuali afferenti al trattamento dei dati personali (contratti con i Contitolari e/o con i Responsabili del trattamento).
- a chi si avvicina per la prima volta all'argomento e cerca una guida completa dal taglio operativo.

2. Prerequisiti per la lettura

Per poter comprendere meglio questo testo è necessaria la dimestichezza con la normativa sulla tutela dei dati personali ed in particolare con il REG.EU. 2016/679

e con i Provvedimenti del Garante. Utile anche la conoscenza della Linea Guida sul DPO del 13 dicembre 2016 emendata il 5 aprile 201 ed il Manuale T4DATA per i DPO approvato dalla Commissione nel luglio 2019. Sono anche utili competenze in merito a: Sistemi di gestione della protezione dei dati personali e della sicurezza delle informazioni, tecniche di audit, risk management.

Riguardo alle norme tecniche, si ricorda che le versioni citate ed utilizzate nel testo sono quelle in vigore al momento della redazione di esso In caso di pubblicazione di nuove edizioni confidiamo nel buonsenso del lettore affinché sappia collocare le parti nel giusto contesto temporale.

Infine, può essere molto utile avere già un'esperienza come Responsabile della protezione dei dati personali o come Referente Privacy, aver operato all'interno di un team privacy o come auditor di conformità legislativa e/o sistemi di gestione.

3. Ambito di trattazione

Il testo si occupa di approfondire aspetti relativi al ruolo del DPO conformemente a quanto previsto dagli artt. da 37 a 39 del REG.EU. 2016/679, in particolare, mediante un taglio pratico, vuole mettere in luce le attività che quotidianamente pone in essere il DPO. Il testo, si occupa, anche dell'aggiornamento del DPO ed infine, prevede una serie di Modelli di atti (capitolo n. 6) che il DPO deve redigere durante il proprio incarico. Ciascun modello viene introdotto da una breve spiegazione sia in merito a quando utilizzare quel determinato documento sia sul contenuto dello stesso.

I Modelli provengono da esperienza diretta sul campo degli autori che rivestono tutti ruolo di DPO in contesti completamente diversi ma afferenti a realtà note a livello nazionale o internazionale. La parte pratica e quella teorica si alternano, quindi, in modo coerente ed, entrambe, hanno pari dignità all'interno del testo.

Benché gli autori abbiano profuso rilevanti energie nella redazione dei Modelli, sono ben consapevoli, che essi possano sempre essere arricchiti e migliorati anche perché come i DPO sanno bene che "*la realtà è sempre più complessa della teoria*".

Gli esempi presentati, quindi, non sono né semplici né banali in quanto il ruolo del DPO richiede di affrontare una elevata complessità a tutela di tutte le parti interessate. Ovviamente i lettori potranno trarre conclusioni diverse da quelle presentate dagli autori e/o soluzioni alternative, anche sulla base del contesto nel quale operano e/o derivanti dall'evoluzione normativa e dei Provvedimenti.

Il testo, si pone, come finalità, quelle di stimolare l'approfondimento sul ruolo del DPO, suscitare nuove riflessioni in grado di arricchire la dialettica su tale nuova figura nonché essere una base di partenza per incentivare comportamenti virtuosi, azioni in grado di limitare le violazioni di dati personali nonché per promuovere la redazione di documenti sempre più completi.

4. Esclusioni

Il testo non ha per oggetto il Regolamento europeo nel suo complesso, ma approfondisce la sola parte relativa agli articoli aventi ad oggetto il ruolo del DPO. Ovviamente, altri articoli e la normativa italiana in materia di protezione dei dati sono trattati nella misura in cui risultano essere funzionali alla tematica in oggetto.

5. Suggerimenti e commenti

I contenuti sono destinati ad evolversi continuamente anche in considerazione della recente introduzione di tale figura nel nostro panorama normativo, pertanto, ogni suggerimento e segnalazione al testo che gli autori possono ricevere dai propri lettori è preziosa e fonte di riflessione.

6. Struttura

Segue un'anticipazione sintetica dei contenuti del testo. Infine saranno indicate le scelte terminologiche: si è cercato di privilegiare la chiarezza didattica e di preferire termini italiani, quando di identico significato a quelli inglesi.

6.1. Sintesi dei contenuti

Il Testo è strutturato ripercorrendo gli artt. da 37 a 39 del REG.EU. 2016/679 e nello specifico:

Capitolo 1: Il Ruolo Soggettivo del DPO
Capitolo 2: La posizione del DPO all'interno dell'Organizzazione
Capitolo 3: I compiti del DPO
Capitolo 4: L'Etica del DPO
Capitolo 5: L'attività del DPO e gli Standard Iso 27701:2019 e BS 10012:2017
Capitolo 6: L'accountability del DPO rispetto al titolare del trattamento
Capitolo 7: L'aggiornamento in concreto del DPO: Provvedimenti delle Autorità Garanti e Giurisprudenza
Capitolo 8: Le Sanzioni

Riguardo alla struttura del testo, il lettore incontrerà all'interno di ciascun capitolo diverse tipologie di contenuti e di stili che possono avere sia un taglio legale sia organizzativo.

6.2. Modelli e casi

Il testo è corredato da Modelli commentati con note (riportate in corsivo per differenziarle dal testo) ogni Modello è introdotto da una breve spiegazione volta alla comprensione del documento.

Tale aspetto per gli autori è un punto di forza del Testo, in quanto, alla teoria è stata coniugata la pratica che ha trovato concretizzazione in detti modelli.

Nel testo sono presenti anche alcuni casi tratti da realtà in cui operano gli autori volti ad approfondire aspetti specifici.

6.3. Note terminologiche

Il "Regolamento concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati" sarà indicato nel seguito come "Regolamento europeo", oppure con la sigla REG.EU. 2016/679.

Nel testo, con l'espressione "normativa privacy" si intende l'insieme delle norme rilevanti in materia di protezione dei dati personali emanate dagli Stati dello Spazio Economico Europeo, incluso il REG.EU. 2016/679 e la normativa nazionale, in particolare il Codice Privacy aggiornato al d.lgs. n. 101/2018, nonché, in ogni tempo, ogni Linea Guida, Provvedimenti del Garante per la protezione di dati, Regolamenti connessi, Codice o Provvedimento rilasciati o emessi dagli Organi competenti o da altre Autorità di controllo dei citati Stati.

Nel testo non sono utilizzati termini particolari, tuttavia, sono presenti, in alcuni casi, note per fornire un'adeguata spiegazione al termine utilizzato.

Nel testo, infine, sono citate diverse funzioni, una di queste è il vertice dell'Organizzazione. Tale funzione che il REG.EU. 2016/679 associa al Titolare del trattamento [1] può essere ricoperta da soggetti diversi: Organo di Governo, Consiglio di Amministrazione, Vertice gerarchico, Amministratore Unico, Amministratore Delegato, altro Soggetto con delega da parte dell'Organo di Governo, Rappresentante Legale, Direzione Generale. Per uniformare è stato usato il termine "Titolare del trattamento".

Si noti, in ultimo, che gli autori per lo più citano il Titolare del trattamento, tuttavia, le considerazioni svolte per quest'ultimo valgono anche per il Responsabile del trattamento.

---

[1] Art. 4 «Titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

6.4. Il ciclo PDCA

Il ciclo PDCA Plan-Do-Check-Act (indicato anche come Ciclo di Deming) è un modello in quattro fasi per supportare ed attuare il cambiamento continuo. Il ciclo PDCA è considerato uno strumento di programmazione di progetto e come tale è utilizzato anche per tenere sotto controllo l'evolversi delle attività dalla pianificazione fino alla standardizzazione.

I passaggi principali prevedono:

- P-Plan Pianificare – riconoscere un'opportunità e pianificare un cambiamento;
- D-Do Eseguire – mettere in atto il cambiamento;
- C-Check Verificare – analizzare i risultati del cambiamento e identificare ciò che si è appreso;
- A-Act Agire – rendere il cambiamento parte integrante dei processi dell'Organizzazione.

Se il cambiamento non ha dato i risultati sperati il ciclo va modificato e ripetuto. Quanto si è appreso deve essere alla base per la pianificazione di nuovi e continui miglioramenti.

Il ciclo PDCA è alla base anche dello stesso Regolamento Europeo, per quanto ciò non risulti in modo evidente e, più in generale, è un elemento fondamentale per gestire un approccio basato sull'accountability ovvero per "*... l'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento) ...*" [2].

Gran parte dei Modelli presentati nel volume [3] si basano sul modello PDCA, per questa ragione gli autori hanno ritenuto di presentarlo nella parte introduttiva del testo. Gli autori raccomandano ai DPO di fare loro tale strumento in quanto, oltre ad essere conosciuto a livello internazionale ed essere di semplice ed immediata applicazione, esso permette, tramite una logica ferrea, di tenere sotto controllo i numerosi aspetti che il DPO deve presidiare.

[2] Estratto da Garante per la protezione dei dati "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali".

[3] Ad esempio: i verbali del DPO, i piani di formazione e quelli di audit.

Capitolo 1

IL RUOLO SOGGETTIVO DEL DPO

Sommario: 1.1. L'Ufficiale della Protezione dei Dati – il DPO. – 1.2. Requisiti del DPO: le precisazioni delle Autorità e della Giurisprudenza. – 1.3. La nomina obbligatoria del DPO. – 1.3.1. La durata dell'incarico del DPO. – 1.3.2. L'attività principale dell'Organizzazione. – 1.4. DPO interno o esterno? Pro e contro delle due ipotesi. – 1.5. Le sanzioni delle Autorità di Controllo in caso di mancata nomina del DPO. – 1.6. Un unico DPO per più Organismi. – 1.7. Sintesi del "*Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico*". – 1.8. Pubblicazione e comunicazione dei dati di contatto del DPO e la Sanzione dell'Autorità di Amburgo. – 1.9. DPO persona Giuridica: l'incarico deve essere conferito ad un lavoratore subordinato della stessa Società o, anche, ad un consulente esterno? La Sentenza del TAR Puglia n. 1468/2019 e l'intervento del Garante. – 1.10. Il DPO può essere considerato un autorizzato ai sensi dell'art. 2-quatordecies Codice Privacy? – 1.11. Nel caso in cui non sia nominato un DPO chi svolge le attività previste dall'art. 39 REG.EU. 2016/679?

1.1. L'Ufficiale della Protezione dei Dati – il DPO

Il Data Protection Officer – DPO – o Responsabile della Protezione dei Dati – RPD – come da traduzione italiana – è una funzione istituita dal Regolamento Europeo n. 2016/679. Ruoli analoghi erano già presenti in Europa prima dell'entrata in vigore del REG.EU. 2016/679, tuttavia non erano mai stati formalizzati da alcuna normativa a livello europeo.

Il Considerando 97 [1] introduce il contenuto degli artt. da 37 a 39 del Regolamento dedicati alla figura del Data Protection Officer.

---

[1] Considerando 97: "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

La funzione del DPO è disciplinata all'interno del Capo IV rubricato "Titolare del trattamento e Responsabile del trattamento". È interessante notare che tale collocazione esemplifica il principio di responsabilizzazione – accountability – che costituisce uno dei fulcri del Regolamento. Il Titolare, infatti, deve attuare le misure che reputa più opportune al fine di garantire la protezione dei dati personali trattati e deve essere sempre nella condizione di poter dimostrare di aver adottato misure adeguate ed efficaci. Secondo tale principio, il Titolare e il Responsabile del trattamento si assumono la responsabilità di nominare o meno il DPO – ad eccezione dei casi obbligatori previsti dall'art. 37 par. 1 del REG.EU. 2016/679 – quindi, di individuare la figura che risulta maggiormente idonea ad esercitare tale funzione. Infatti, il Regolamento Europeo non stabilisce precisi requisiti necessari ai fini dell'esercizio del ruolo di DPO, lasciando, quindi, "carta bianca" ai Titolari e ai Responsabili del Trattamento.

Ciò non esclude che il REG.EU. 2016/679 individui nella suddetta figura una funzione fondamentale nella protezione dei dati personali, prevedendo specifiche disposizioni in merito alla designazione, alla posizione ed ai compiti ad esso attribuiti.

1.2. Requisiti del DPO: le precisazioni delle Autorità e della Giurisprudenza

Come anticipato, in un'ottica di accountability, il REG.EU. 2016/679 non individua requisiti puntuali che il DPO deve possedere. L'art. 37 denominato "Designazione del Responsabile della protezione dei dati", oltre a precisare che tale figura può essere sia interna all'Organizzazione del Titolare (o Responsabile del Trattamento) sia una persona fisica o giuridica che svolge il ruolo sulla base di un contratto di servizi, prevede esclusivamente che il DPO sia "*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'art. 39*" [2]. Pertanto, spetta al Titolare o al Responsabile individuare, in concreto, tali qualità professionali. Il Considerando n. 97 rileva, inoltre, che "*il Titolare o il Responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in*

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".

[2] Cfr. REG.EU. n. 679/2016, art. 37.

materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento" [3].

Le Linee Guida sui Responsabili della Protezione dei Dati, "WP 243 rev. 01", analizzano le conoscenze specialistiche e le competenze che deve possedere il DPO.

Con riferimento al livello delle conoscenze specialistiche, l'ex WP29 [4] ribadisce che non sono previsti criteri tassativi: il Titolare che intende nominare un DPO deve *in primis* valutare, in concreto, la complessità della propria organizzazione, la quantità di dati personali trattati e l'eventuale trasferimento – sistematico od occasionale – di tali dati al di fuori dell'Unione Europea.

È inevitabile, quindi, che un'accurata e ragionata individuazione del DPO non può prescindere da una preliminare analisi del contesto organizzativo, delle categorie di dati personali trattati e di ulteriori eventuali complessità inerenti il trattamento ad opera del Titolare.

In merito alle qualità professionali, le Linee Guida sottolineano innanzitutto la necessaria conoscenza – da parte del DPO – delle prassi e della normativa nazionale ed europea. Nello specifico si evidenzia "*un'approfondita conoscenza del RGPD*" in materia di protezione dei dati personali. A tale proposito l'ex WP29 riconosce l'importanza di una "*formazione adeguata e continua*" rivolta ai DPO da parte delle Autorità di Controllo nazionali.

Tuttavia, oltre alla conoscenza della normativa e della prassi, il DPO – affinché possa svolgere al meglio la propria funzione – dovrebbe conoscere al meglio la realtà organizzativa del Titolare, ovvero dovrebbe essere pienamente consapevole ed edotto in merito al settore di attività del Titolare. Egli dovrebbe, altresì, avere contezza di tutti i trattamenti effettuati all'interno dell'Organizzazione, nonché dei sistemi informativi adottati e delle specifiche esigenze di sicurezza del Titolare. Ad esempio, nel caso in cui il DPO svolga la sua funzione per un ente pubblico, è opportuno che conosca le norme e i procedimenti amministrativi tipici del settore.

Infine, le Linee Guida esaminano la capacità del DPO di assolvere ai propri compiti. Tale aspetto afferisce sia alle qualità personali sia alle conoscenze del DPO, sia al suo status all'interno della realtà in cui svolge i compiti affidatigli.

In riferimento alle qualità personali, il DPO dovrebbe possedere "*integrità ed elevati standard ideologici*", dovrebbe perseguire l'osservanza del REG.EU. 2016/679 e dovrebbe promuovere la cultura della protezione dei dati.

Il DPO dovrebbe, altresì, sensibilizzare il Titolare in merito all'applicazione dei principi fondamentali del Regolamento, al rispetto dei diritti degli interessati, alla protezione dei dati by design e by default, alla tenuta dei registri delle attività di

---

[3] Cfr. REG.EU. n. 679/2016, Considerando n. 97.

[4] Il WP29 – Working Party 29– era un organo consultivo disciplinato dall'art. 29 della Direttiva 95/46/CE. Con l'entrata in vigore del REG.EU. n. 679/2016, il WP29 è stato sostituito dal Consiglio Europeo per la Protezione dei Dati – EDPB.

trattamento, alla sicurezza dei trattamenti, alla notifica al Garante e alla comunicazione agli interessati delle violazioni di dati personali (Data Breach).

L'Autorità Garante italiana è intervenuta in merito ai requisiti che il DPO deve possedere nell'ambito del riscontro ad un quesito posto da un'Azienda Ospedaliera. Il Garante, richiamando il contenuto delle Linee Guida, sottolinea la delicatezza dei dati personali trattati dall'Azienda stessa e, pertanto, consiglia di designare un DPO particolarmente abile ed esperto in merito alla gestione dei trattamenti di dati sanitari e genetici. Inoltre, l'Autorità italiana evidenzia che, ad oggi, non è stato previsto un vero e proprio Albo per i Responsabili della Protezione dei Dati e che le eventuali certificazioni delle competenze – ad oggi esistenti – non sono propedeutiche all'esercizio della funzione del DPO. Tali certificazioni dimostrano esclusivamente la partecipazione ad attività formative terminate con il superamento di un esame finale, ma non rappresentano in alcun modo una sorta di abilitazione all'esercizio della funzione del DPO né, conclude il Garante, "*possono sostituire in toto la valutazione della p.a. nell'analisi del possesso dei requisiti del RPD necessari per svolgere i compiti da assegnarli in conformità all'art. 38 del Regolamento (UE) 2016/679.*" [5].

Pertanto, il conseguimento da parte del DPO di certificazioni, master, corsi professionalizzanti non può essere posto quale requisito per l'esercizio della funzione del DPO, bensì è idoneo esclusivamente a dimostrare il possesso di specifiche conoscenze in materia. Spetta, quindi, al Titolare valutare e verificare – in ottica di accountability – l'adeguatezza del DPO rispetto alla complessità dei dati personali trattati, ai trattamenti effettuati, alla struttura organizzativa ed alle misure di sicurezza adottate.

L'Autorità Garante della Concorrenza e del Mercato con l'atto di segnalazione n. AS201636 del 2 gennaio 2020 ha ribadito che "*Rispetto ai requisiti che il RPD deve possedere, è opportuno chiarire che la normativa in vigore non fa riferimento a specifici titoli di studio, né richiede iscrizioni agli albi professionali.*" [6]. In particolare, richiamando quanto stabilito dal REG.EU. 2016/679 e statuito dalle Linee Guida elaborate dall'ex WP29, la predetta Autorità ha evidenziato come la pretesa di alcune Pubbliche Amministrazioni avente ad oggetto l'iscrizione all'albo professionale degli avvocati quale requisito indispensabile per ricoprire il ruolo di DPO, risulti discriminatoria e non giustificata. Infatti, il predetto requisito non dimostra in alcun modo il possesso di specifiche competenze in materia ed esclude ingiustificatamente soggetti che, pur essendo esperti in materia di protezione dei dati personali, non sono iscritti al predetto Albo. In conclusione, l'Autorità invita le Pubbliche Amministrazioni a valutare "*con attenzione i requisiti da inserire nei propri bandi per la selezione dei RPD al fine*

---

[5] Cfr. "*Quesiti in materia di certificazione delle competenze ai fini della prestazione di consulenza in materia di protezione dei dati personali*", Doc-Web n. 7057222 del 28 luglio 2017.

[6] Cfr. AS 201636 del 2 gennaio 2020 dell'Autorità Garante della Concorrenza e del Mercato.

di evitare restrizioni all'accesso alle selezioni che possano risultare sproporzionate e ingiustificate.".

Poco dopo l'entrata in vigore del REG.EU. 2016/679, anche l'Autorità Giudiziaria amministrativa è intervenuta rispetto ai requisiti propri del DPO. Il TAR del Friuli Venezia Giulia, con sentenza del 13 settembre 2018, si è pronunciato in merito al valore di un titolo certificativo "Auditor/Lead Auditor per i Sistemi di Gestione per la Sicurezza delle Informazioni secondo la norma ISO/IEC/27001" – richiesto da un'Azienda Sanitaria nell'ambito di una procedura di selezione pubblica per l'affidamento dell'incarico di DPO. Il TAR, uniformandosi al contenuto delle Linee Guida, ha confermato che tale certificazione non equivale ad un'abilitazione all'esercizio della funzione del DPO, in primo luogo, poiché il titolo certificativo sopra richiamato attiene principalmente all'attività di impresa e, in secondo luogo, poiché "*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 mediante la procedura selettiva intrapresa dall'Azienda, il cui profilo, per le considerazioni anzidette, non può che qualificarsi come eminentemente giuridico.*" [7]. Pertanto il TAR ha concluso che la suddetta certificazione non può essere considerata quale requisito di ammissione alla procedura di selezione, non costituendo un titolo formativo o abilitante, bensì trattandosi di un mero titolo curriculare.

1.3. La nomina obbligatoria del DPO

L'art. 37 del REG.EU. 2016/679 individua innanzitutto i casi in cui il Titolare o il Responsabile del trattamento sono obbligati a designare un DPO, tenendo presente che ulteriori casi di nomina obbligatoria possono essere previsti dal diritto dell'Unione Europea o degli Stati membri [8].

In primo luogo, le Autorità pubbliche e gli organismi pubblici devono nominare un DPO, ad eccezione delle Autorità giudiziarie nell'esercizio delle funzioni giurisdizionali.

Il REG.EU. 2016/679 non definisce le nozioni di "*Autorità Pubbliche*" e di "*organismi pubblici*", tuttavia l'ex WP29 viene in soccorso affermando che la definizione dei predetti concetti si deve trarre dalla normativa nazionale degli Stati membri.

Il Garante italiano chiarisce che "*in ambito pubblico, devono ritenersi tenuti alla designazione di un RPD i soggetti che ricadevano nell'ambito di applicazione degli artt. 18-22 del Codice, che stabilivano le regole generali per i trattamenti ef-*

[7] Cfr. TAR Friuli Venezia-Giulia, sentenza del 13 settembre 2018, n. 287.

[8] Cfr. Reg. UE n. 2016/679, art. 37 par. 4.

fettuati dai soggetti pubblici (ad esempio, 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 ecc.)." [9].

Inoltre, il d.lgs. n. 50/2016 – c.d. Codice dei Contratti Pubblici – definisce l'organismo pubblico all'art. 3, comma 1, lett. d), ricomprendendo nella nozione "*qualsiasi organismo, anche in forma societaria istituito per soddisfare specificatamente esigenze di interesse generale, avente carattere non industriale o commerciale; dotato di personalità giuridica; la cui attività sia finanziata in modo maggioritario dallo Stato, dagli enti pubblici territoriali o da altri organismi di diritto pubblico oppure la cui gestione sia soggetta al controllo di questi ultimi oppure il cui organo d'amministrazione, di direzione o di vigilanza sia costituito da membri dei quali più della metà è designata dallo Stato, dagli enti pubblici territoriali o da altri organismi di diritto pubblico*" [10].

Inoltre, sebbene non rientri nei casi obbligatori appena esaminati, l'ex WP29 ritiene opportuna la nomina del DPO anche da parte di "*organismi privati incaricati di funzioni pubbliche o che esercitano pubblici poteri*".

Alla luce di quanto illustrato sino ad ora, il REG.EU. 2016/679 prevede la designazione obbligatoria del DPO per le amministrazioni e gli enti pubblici, ma, come già indicato, la lett. a) dell'art. 37 prevede un'eccezione, ed invero se il trattamento è effettuato da una Autorità giudiziaria (ad esempio Tribunali, Procure, ecc.) non sussiste l'obbligo di nomina. Disposizione che, a contrario, può essere letta anche dal punto di vista della "facoltatività" della suddetta nomina.

A tal proposito è intervenuto il d.lgs. n. 101/2018 che, tra le varie disposizioni di adeguamento, all'art. 2-sexiesdecies prevede che "*Il responsabile della protezione dati è designato, a norma delle disposizioni di cui alla sezione 4 del capo IV del Regolamento, anche in relazione ai trattamenti di dati personali effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni*".

La norma, con tale previsione, quindi, ha assoggettato anche l'Autorità giudiziaria all'obbligo di designazione del DPO da effettuarsi secondo quanto previsto dal GDPR (nello specifico dagli artt. 37, 38 e 39 del Regolamento), in relazione ai trattamenti effettuati nell'esercizio delle loro funzioni.

Tornando ora alle ipotesi di nomina obbligatoria del DPO previste dall'art. 37 REG.EU. 2016/679, rientrano i casi in cui le attività principali del Titolare o Responsabile del trattamento riguardano "*trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala*".

---

[9] Cfr. *Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico (in aggiunta a quelle adottate dal Gruppo Art. 29),* Doc-web n. 7322110, del 15 dicembre 2017.

[10] Cfr. Linee Guida sui Responsabili della Protezione dei Dati, par. 2.1.1.

Anche in tale caso è necessario fare riferimento alla Linee Guida sui Responsabili della Protezione dei Dati al fine di comprendere i concetti di "*attività principali*", "*larga scala*" e "*monitoraggio regolare e sistematico*".

L'ex WP29 rileva innanzitutto che il primo riferimento alle c.d. "*attività principali*" nel REG.EU. 2016/679 è contenuto nel Considerando n. 97.

In ogni caso, le Linee Guida esplicitano chiaramente come le attività principali poste in essere dal Titolare "*riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria*". Pertanto, devono considerarsi attività principali solo "*le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal Titolare del trattamento o dal Responsabile del trattamento*.".

È necessario, quindi, distinguere i trattamenti dei dati personali effettuati con la finalità di perseguire l'obiettivo del Titolare dai trattamenti meramente accessori, questi ultimi estranei rispetto all'attività primaria del Titolare.

Al proposito, il seguente esempio può essere chiarificatore: un'azienda sanitaria tratta i dati personali dei propri dipendenti anche al fine di erogare la retribuzione. Tuttavia, l'erogazione del salario non può essere considerata l'attività principale dell'azienda sanitaria, bensì una mera attività accessoria funzionale allo svolgimento dell'attività principale ed al perseguimento degli obiettivi di tale azienda, ovvero l'erogazione di servizi volti alla tutela della salute.

Con riferimento alla nozione di "*larga scala*", l'ex WP29 cita il Considerando n. 91 che fornisce alcune indicazioni generiche in merito all'individuazione di trattamenti su larga scala. In particolare, tale Considerando evidenzia che il trattamento – per considerarsi su larga scala – deve riguardare "*una notevole quantità di dati personali a livello regionale, nazionale e sovranazionale*" e che dallo stesso dovrebbe derivare un rischio elevato per i diritti e le libertà degli interessati, connesso, a titolo meramente esemplificativo, alla sensibilità dei dati personali trattati o all'utilizzo di nuove tecnologie.

Tuttavia, anche con le predette indicazioni, risulta particolarmente complesso quantificare con esattezza il numero di dati personali trattati o il numero di interessati in modo da stabilire con precisione se il trattamento preso in considerazione possa essere definito su "*larga scala*". L'ex WP29 prevede la possibilità di elaborare, in futuro, standard da applicare al fine di meglio circoscrivere i trattamenti di dati personali che possano essere considerati su "*larga scala*".

Nel frattempo, il Titolare può utilizzare i seguenti elementi per comprendere se pone in essere o meno un trattamento su "*larga scala*":

1. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
2. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
3. la durata, ovvero la persistenza, dell'attività di trattamento;
4. la portata geografica dell'attività di trattamento [11].

[11] Cfr. Linee Guida su Responsabili della Protezione dei Dati, par. 2.1.3.

L'ex WP29 riporta nelle Linee Guida sui Responsabili della Protezione dei dati, alcuni esempi di trattamenti su "*larga scala*" [12], e riprende quanto sancito dal Considerando n. 91 in merito ai trattamenti che non sono da considerarsi su larga scala e precisamente: il trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario; il trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Infine, le Linee Guida approfondiscono il concetto di "*monitoraggio regolare e sistematico*" degli interessati.

Il Considerando n. 24 esamina il "*monitoraggio del comportamento*" degli interessati, ritenendo, all'uopo, opportuno valutare se gli interessati sono tracciati in internet con varie modalità, in particolare attraverso la profilazione dei dati personali. Sebbene il Considerando n. 24 usi una terminologia differente rispetto all'art. 37 del REG.EU. 2016/679, si può dedurre che il tracciamento e la profilazione online siano da considerarsi a tutti gli effetti un monitoraggio rilevante ai fini della nomina del DPO.

L'ex WP29 individua poi diversi significati da attribuire all'aggettivo "*regolare*" e precisamente un monitoraggio si intende regolare se avviene in modo continuo o con intervalli definiti; se è ricorrente o ripetuto a intervalli costanti; se avviene in modo costante o a intervalli periodici.

L'aggettivo "*sistematico*", invece, indica che il trattamento è effettuato per sistema, ovvero in modo predeterminato, organizzato o metodico, in riferimento ad un progetto complessivo di raccolta di dati o ad una strategia [13].

L'ex WP29 conclude la sua analisi fornendo alcuni esempi di attività che possono costituire un "*monitoraggio regolare e sistematico*" di interessati [14].

---

[12] Cfr. Linee Guida su Responsabili della Protezione dei Dati, par. 2.1.3: "*Alcuni esempi di trattamento su larga scala sono i seguenti:*

– trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;

– trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);

– trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un Responsabile del trattamento specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;

– trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;

– trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;

– trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.".

[13] Cfr. Linee Guida su Responsabili della Protezione dei Dati, par. 2.1.4.

[14] Cfr. Linee Guida su Responsabili della Protezione dei Dati, par. 2.1.4: "*Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valuta-*

1.3.1. La durata dell'incarico del DPO

Stabilita la necessità o la volontà di nominare un DPO, ogni Organizzazione deve definire la durata dell'incarico di quest'ultimo. È opportuno che tale arco temporale copra almeno due – tre anni in modo da dare una continuità all'operato dello stesso. Un arco temporale più ridotto, pari ad esempio ad un anno, renderebbe complesso poter impostare un'attività di medio termine che è importante per il presidio dell'attività.

Tuttavia, archi temporali più lunghi di un triennio potrebbero determinare, in caso di DPO esterni, la difficoltà, per l'Organizzazione, di rimuovere lo stesso nel caso di inadempienze. L'Organizzazione per garantire l'indipendenza del DPO di fatto può esautorarlo quasi esclusivamente al termine del proprio mandato o in presenza di gravi inadempienze.

Gli autori hanno potuto constatare anche casi in cui il DPO esterno era stato incaricato per un periodo non definito, tale prassi, tuttavia, non si ritiene assolutamente adeguata.

1.3.2. L'attività principale dell'Organizzazione

Per la determinazione dell'attività principale dell'Organizzazione che richiede un trattamento di dati che richiede la presenza del DPO come previsto dall'art. 37 REG.EU. 2016/679, si possono formulare alcune valutazioni qualitative:

- l'incidenza dell'attività/delle attività che richiedono tale figura in percentuale rispetto al fatturato;
- l'incidenza dell'attività/delle attività che richiedono tale figura in percentuale rispetto al numero complessivo degli interessati;
- l'incidenza dell'attività/delle attività che richiedono tale figura in percentuale al numero complessivo di dati trattati.

Qualche esempio può aiutare:

- l'Organizzazione che sviluppa software e fornisce assistenza post-vendita per ambiti diversi tra cui anche quello sanitario e quest'ultimo incide sul fatturato per il 30% è raccomandato che nomini un DPO;
- caso analogo al precedente ma l'incidenza sul fatturato è pari al 5% deve valutare la nomina di un DPO;

---

zione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.".

- caso analogo al precedente, ma il numero dei dati trattati per lo sviluppo del software in ambito sanitario sono pari al 60% del complesso dei dati trattati (in alternativa il numero degli interessati sono pari al 70% degli interessati trattati) deve nominare un DPO.

1.4. DPO interno o esterno? Pro e contro delle due ipotesi

Dopo aver analizzato i casi di nomina obbligatoria del DPO, risulta opportuno fornire alcune indicazioni di carattere qualitativo sull'opportunità o meno di nominare un DPO interno piuttosto che esterno, lasciando, tuttavia, al lettore le conclusioni da trarre a proposito. Il peso da dare alle relative argomentazioni dipende infatti, in modo rilevante, dal contesto in cui si opera. Gli autori, in questo caso, si limitano a fornire spunti di riflessione senza giungere ad alcuna conclusione.

Certo è che di solito, gli elementi a favore di un DPO interno sono corrispondenti a quelli a sfavore del DPO esterno.

Aspetti a sostegno del DPO interno

- Conosce, in modo approfondito, i profili organizzativi e gestionali dell'Organizzazione, pertanto, è facilitato nel venire a conoscenza e nel reperire informazioni.
- È, di norma, più facilmente reperibile.

Aspetti a sostegno del DPO esterno

- La posizione di autonomia è più facilmente garantita così come l'assenza di pregiudizi e preconcetti nei confronti dell'Organizzazione, aree/Business Unit/uffici, collaboratori, fornitori e partner.
- Data la posizione autonoma il DPO è facilitato a segnalare criticità anche in carico a figure apicali.
- Una serie di costi, possono essere a carico del DPO (es. formazione[15], forme assicurative).
- Il cambio del DPO, inevitabilmente più frequente, porta a innovare le modalità secondo le quali l'attività viene svolta, costringendo quindi l'Organizzazione a ripensare criticamente le misure poste in essere.
- Nel caso di rinuncia al ruolo il rapporto di collaborazione si interrompe senza lasciare ulteriori strascichi, in primis, nei rapporti umani.

---

[15] L'art. 32, par. 2, Reg. UE 2016/679 indica che il Titolare del trattamento ha in carico di fornire al DPO "… le risorse necessarie … per mantenere la propria conoscenza specialistica".