Anno 6, n. 11 – LUGLIO 2018
Nuova Etica Pubblica
Rivista dell'Associazione Etica PA

# Il Data Protection Officer quale garante interno alle organizzazioni del trattamento dei dati



*di Vincenzo Pensa*
*Direttore dei Sistemi Informativi e dell'Innovazione in ACI e Segretario Generale di CIDA FC - Sez. ACI*

Dal 25 maggio scorso il **GDPR (Regolamento Generale sulla Protezione dei Dati,** emanato con delibera UE n. 679 dell'anno 2016 – clicca qui per il testo in italiano) esplica pienamente i propri effetti nel nostro ordinamento e con esso abbiamo iniziato a prendere confidenza con una nuova figura che viene istituita dalla norma: il **Responsabile della Protezione dei Dati** (RPD).

A conti fatti, tuttavia, non ha avuto molta fortuna l'acronimo RDP visto che, infatti, la figura professionale continua ad essere nota a tutti come **DPO (Data Protection Officer)**, denominazione internazionale che facilita le comunicazioni tra i vari Paesi europei tutti soggetti alla medesima disciplina sulla protezione dei dati personali.

Il DPO costituisce a tutti gli effetti una delle principali novità introdotte dalla nuova normativa anche se non tutte le organizzazioni sono tenute a nominarlo. Lo sono, senza entrare troppo nei dettagli, le amministrazioni pubbliche e le organizzazioni private che abbiano quali attività principali il monitoraggio sistematico o che trattano su larga scala particolari dati personali.

La nomina del DPO è quindi uno dei primissimi adempimenti che le amministrazioni pubbliche e gli altri soggetti che vi sono tenuti, avrebbero dovuto assicurare entro il 25 maggio 2018, anche perché il DPO, con il suo ruolo di guida e consulenza, dovrebbe svolgere una funzione di motore propulsivo in grado di portare l'organizzazione verso la completa osservanza del nuovo assetto normativo.

Come per gli altri adempimenti introdotti dal GDPR lo stato dell'arte, peraltro di non semplice rilevazione, stante la gran quantità dei soggetti che sarebbero tenuti a nominare il DPO, ad oggi presenta un quadro estremamente diversificato e disomogeneo. Qualcuno confida in un minor rigore dei **controlli nella fase iniziale di applicazione della norma**, ma si tratta di un atteggiamento estremamente rischioso e improvvido, foriero dunque di possibili gravi conseguenze che non devono essere sottovalutate.

Ciò detto, giova ricordare che nelle sue **Linee guida sui responsabili per la protezione dei dati** (vedi qui il testo) il WP29 raccomanda comunque ("può risultare utile") la designazione di un DPO anche da parte di quelle organizzazioni che non sarebbero tenute a farlo.

Il WP29 è il "**Gruppo di lavoro articolo 29**" (Working Party article 29 o WP29, appunto perché previsto dall'art. 29 della direttiva europea 95/46), oggi sostituito dall'European Data Protection Board, o Comitato europeo per la protezione dei dati (previsto dall'art. 68 del Regolamento) e composto da un rappresentante della varie autorità nazionali, che al DPO ha dedicato specifiche Linee guida pubblicate nell'aprile dello scorso anno.

Ma chi è e a cosa serve il DPO?

Per intendere a pieno funzioni e ruolo della nuova figura occorre brevemente introdurre un altro concetto importante e basilare per il GDPR: **il principio dell'*accountability*.** Il termine *accountability* potrebbe essere tradotto con "responsabilizzazione" ma, come per il DPO, anche qui è forse meglio mantenere il termine inglese, visto che si tratta per l'appunto di un concetto più consueto e finora meglio definito in ambito nord europeo e su cui in Italia (sistema imperniato sul diritto codificato) si è avuta finora poca dimestichezza.

**L'intero impianto del GDPR si basa sul principio della responsabilizzazione del titolare del trattamento** (ed in misura minore del responsabile del trattamento), ai quali compete l'onere e la relativa responsabilità, di individuare il **modo migliore per proteggere i dati personali.** In buona sostanza non abbiamo più un insieme di norme puntuali che prevedono precise prescrizioni e adempimenti che devono essere rispettati ed eseguiti, quanto piuttosto una serie di principi che devono essere osservati e obiettivi che devono essere perseguiti. Il come dipende però da ogni singolo Ente o Azienda che dovrà autonomamente adottare e porre in essere tutte quelle attività che riterrà utili per il perseguimento dei predetti obiettivi.

Di conseguenza cambia anche il ruolo dell'Autorità di controllo che nei suoi interventi valuterà a posteriori se quanto posto in essere dagli Enti e dalle Aziende garantisce o meno il rispetto della norma e, soprattutto, la tutela dei diretti interessati.

A questo punto si comprende meglio l'importanza della funzione del DPO cui compete l'individuazione delle misure organizzative e procedurali più idonee per la tutela e la garanzia dei dati; una **figura che assume il ruolo di "garante" interno con il compito di sorvegliare l'applicazione del GDPR nella propria organizzazione e fornire un supporto consulenziale** al titolare del

trattamento ed al responsabile del trattamento, le altre figure alle quali il GDPR attribuisce una particolare rilevanza. Questo compito in passato veniva assicurato direttamente e centralmente dall'Autorità di controllo principalmente tramite l'emanazione di pareri.

Con il nuovo impianto normativo, l'Autorità di controllo viene quindi ad assumere precipuamente un **ruolo di regolatore generale e di controllore**. Per tutte le modalità di applicazione operative delle disposizioni per la protezione dei dati personali, le organizzazioni invece si relazionano direttamente con il proprio DPO, il quale funge anche quale punto di contatto con l'Autorità di controllo.

Il ruolo del DPO quale "garante" interno alle organizzazioni è confermato dalla sua irresponsabilità per l'inosservanza degli obblighi in materia di protezione dei dati, per i quali rispondono il titolare del trattamento ed il responsabile del trattamento.

In funzione di tale posizione di "garante", il GDPR si preoccupa di assicurare che il **DPO abbia un ruolo di terzietà ed indipendenza**. Per cui né il titolare né il responsabile del trattamento dovranno dare alcuna istruzione al DPO e, se è un dipendente della organizzazione, dovrà essere messo in condizione di operare in modo indipendente.

Sempre in questa ottica si inserisce la disposizione secondo cui il **DPO riferisce direttamente al vertice gerarchico dell'organizzazione** e deve essere tempestivamente coinvolto in tutte le questioni che riguardano la materia dei dati personali.

Poiché, per ragioni facilmente intuibili, visto che opera con una particolare attenzione rivolta alla tutela degli interessati (che difatti possono contattarlo direttamente, art. 38 par. 4), il DPO potrebbe diventare una figura scomoda all'interno dell'organizzazione e quindi in potenziale contrasto con i desiderata dell'organizzazione stessa, il Regolamento si preoccupa di precisare che il DPO non può essere rimosso né tanto meno penalizzato in termini di incentivazioni e carriera.

Come accennato, naturale corollario della posizione così descritta è la sua terzietà rispetto alle problematiche trattate. La scelta della persona da incaricare non deve pertanto dare adito a possibili conflitti di interesse (art. 38 par. 6).

La questione diventa particolarmente delicata nel caso in cui il DPO sia scelto tra i dipendenti dell'organizzazione di appartenenza in quanto potrà continuare a svolgere altri compiti e funzioni per conto della stessa organizzazione (come ammette espressamente il medesimo art. 38 par. 6), ma tali

compiti e funzioni non potranno essere in conflitto rispetto agli adempimenti che dovranno essere assicurati nella sua funzione di DPO.

Il GDPR non precisa ulteriormente cosa debba intendersi per **conflitto di interessi** e quali siano le casistiche che possono esservi comprese. Sull'argomento si è però soffermato il WP29 che, nelle sue Linee Guida sui responsabili della protezione dei dati, ha precisato che per cogliere i casi di possibile conflitto di interesse, occorre verificare chi abbia la competenza a definire le finalità o modalità di trattamento dei dati personali. Per l'appunto il DPO non deve trovarsi in una posizione che potrebbe consentirgli di esercitare tale potere.

Di conseguenza, non possono assumere la funzione di DPO tutti coloro che occupano ruoli manageriali di vertice all'interno dell'organizzazione. Pertanto, a mero titolo esemplificativo, il ruolo di DPO sarà incompatibile con quella del CIO, di responsabile per le risorse umane, di responsabile commerciale, di responsabile delle unità di produzione o di responsabile finanziario.

Vanno altresì esclusi anche coloro che occupano ruoli gerarchicamente inferiori, ma comunque idonei a metterli in condizione di influire sulla determinazione, sulle finalità o modalità di trattamento dei dati personali.

Al contrario, **la funzione del DPO non è incompatibile con il ruolo di Responsabile della Trasparenza,** essendo questo caratterizzato da terzietà rispetto all'organizzazione.

Non rileva invece la qualifica rivestita all'interno dell'organizzazione, anche se il Garante suggerisce di individuare il DPO tra i dirigenti in considerazione del fatto che esso dovrà rapportarsi direttamente con il vertice gerarchico e con gli altri pari grado.

Un'altra questione degna di nota è quella relativa al fatto di potersi avvalere di un **DPO di nomina esterna. Sia il GDPR che le Linee guida del WP29 non danno infatti nessuna preferenza circa la scelta di nominare un DPO interno piuttosto che esterno**. Ciascuna organizzazione può quindi liberamente sceglierlo tra i dipendenti oppure stipulare un contratto di servizio con un soggetto esterno (art. 37 par. 6). La scelta di un soggetto esterno probabilmente in fase di avvio potrà apparire più agevole in quanto facilita alcuni aspetti, quali quello dell'individuazione di un soggetto dotato di adeguate capacità professionali a volte non presenti all'interno.

Tuttavia **il Garante ha consigliato alle amministrazioni pubbliche di dotarsi di un DPO interno,** non tanto per il rischio che possano essere divulgate informazioni delicate facenti capo all'amministrazione, quanto per la obiettiva complessità delle procedure delle pubbliche

amministrazioni e per la pervasività della funzione che sarà destinata ad interfacciarsi con tutte le altre funzioni interne.

La selezione del DPO da parte delle amministrazioni pubbliche dovrà sempre rispettare i criteri per l'affidamento degli incarichi, quali la pubblicazione di avvisi per la ricezione di manifestazione di interesse per gli esterni e interpelli per gli interni.

Il DPO dovrà possedere adeguate conoscenze e capacità e sarà 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". Questa formulazione del Regolamento che è in effetti piuttosto generica (anche le Linee Guida WP29 non aggiungono molto di più) si comprende con l'intenzione di dare un quadro di riferimento generale adatto alle molteplici casistiche a cui dovrà applicarsi.

Come visto non c'è un titolo di studio o una particolare abilitazione richiesta, la selezione andrà pertanto effettuata caso per caso ed ovviamente un DPO di un'impresa con migliaia di dipendenti dovrà possedere capacità e conoscenze adeguate allo scopo specifico e comunque diverse da quelle di un DPO di un piccolo Comune. E' bene ricordare che **più Enti possono anche accordarsi tra loro per nominare un DPO comune** in ossequio ai principi di semplificazione ed economicità (si pensi ai casi di Comuni limitrofi).

Il Regolamento non ci dice poi come il DPO dovrà in concreto lavorare. Sappiamo che potrà contemporaneamente svolgere altri compiti, compatibilmente con gli impegni e la complessità dell'organizzazione, visto che gli adempimenti relativi ai trattamenti di dati personali avranno comunque la priorità.

Per garantire tale priorità, soprattutto per le organizzazioni più grandi e complesse, sarà certamente utile dotare il DPO di uno staff che possa supportarlo per l'ordinaria gestione operativa. Il GDPR non pone alcun vincolo al riguardo, né le Linee Guida arrivano a prescrivere alcunché, limitandosi a prevedere che il DPO possa essere "supportato da un apposito team se necessario". In ogni caso al DPO dovranno essere assicurate le risorse strumentali e finanziarie necessarie per lo svolgimento dei propri compiti e non andrà nemmeno trascurato un parallelo adeguato percorso formativo.

Va qui ricordato che il Garante, evidentemente consapevole della delicatezza e della complessità del ruolo e delle funzioni, nei colloqui con le amministrazioni è stato più esplicito nel raccomandare **l'esigenza di affiancare al DPO una stabile ed efficiente struttura**. Quanto debba essere articolata e numerosa tale struttura dipende, anche qui, dai singoli casi. Ogni amministrazione farà quindi le proprie valutazioni e dedicherà all'affiancamento del DPO un numero di risorse tale da consentirgli di esercitare il proprio compito con efficienza. Di certo non potranno mancare professionalità con conoscenze nel campo dell'ICT e del settore legale specializzate nel settore della privacy oltre che esperti della specifica attività curata dall'organizzazione.

Il DPO assume quindi un ruolo di guida sui temi della protezione dei dati personali. Ciò non significa che debba assumere decisioni al riguardo. Il DPO infatti, non decide ma consiglia e guida il titolare ed il responsabile del trattamento i quali, sotto la propria responsabilità, potranno anche decidere di discostarsi dalle sue indicazioni.

Questo spiega come mai il DPO non abbia particolari responsabilità che invece ricadono sul titolare e sul responsabile del trattamento cui competono le decisioni finali.

E' peraltro appena il caso di sottolineare come la decisione del titolare o del responsabile del trattamento di discostarsi dalle indicazioni del DPO avrà comunque un suo peso nella successiva valutazione dell'Autorità di controllo, soprattutto qualora si accerti che la condotta del titolare abbia comportato un rischio per i dati personali, ciò anche ai fini dell'applicazione delle sanzioni.

Si prenda per esempio il caso della **valutazione di impatto che il titolare è tenuto ad effettuare prima di procedere a nuovi trattamenti** che potrebbero essere soggetti a particolari rischi e per la quale il DPO svolge un ruolo importante.

Egli infatti partecipa alla procedura di valutazione di impatto fornendo un parere al titolare (il quale è tenuto a consultarsi con lui, art. 35 par. 2) e, nel fornire tale parere, il DPO potrà eventualmente segnalare se dalla valutazione è emerso un rischio residuo elevato, tale da rendere necessaria l'attivazione della consultazione preventiva dell'Autorità di controllo.

Tale **parere non è vincolante per il titolare del trattamento** il quale, sotto la propria responsabilità e secondo il principio dell'*accountability*, potrà discostarsene non consultando l'Autorità la quale ne terrà però conto in un'eventuale fase di controllo.

Nella richiesta di consultazione preventiva dovranno essere indicati i dati di contatto del DPO (art. 36, par. 3, lett. d, nella traduzione italiana indicato con l'insolito nome di "titolare della protezione dei dati". La versione inglese chiarisce tuttavia che si tratta del data protection officer) che resta, come detto, l'interlocutore privilegiato dell'Autorità di controllo (v. anche art. 39, par. 1, lett. e).

In conclusione la figura del DPO fa il suo ingresso nel nostro ordinamento e si annuncia come una positiva novità che potrà essere di grande aiuto alle organizzazioni soprattutto se le stesse sapranno cogliere l'opportunità di realizzare nuovi percorsi e metodologie di lavoro che puntino sulla trasparenza e l'integrazione dei processi interni ponendo al centro delle proprie riflessioni l'obiettivo di curare al meglio l'interesse dei cittadini, siano essi utenti di un servizio pubblico o consumatori di prodotti e servizi offerti dal mercato.

Anno 6, n. 11 – LUGLIO 2018
Nuova Etica Pubblica
Rivista dell'Associazione Etica PA

# La relazione tra GDPR e innovazione digitale

*di Piero De Luca*
*Funzionario Camera dei Deputati*



I dati personali sono al centro della *digital transformation*. Infatti, sentiamo sempre più spesso parlare di auto a guida autonoma, di *smartworking*, di controllo a distanza della propria abitazione e degli elettrodomestici. Il punto fondamentale dell'innovazione è trasformare in servizi innovativi per le persone o relativi alle persone, l'enorme mole di dati che le nuove tecnologie consentono di raccogliere, analizzare, tracciare, condividere e incrociare.

I fatti di cronaca hanno già fatto emergere i rischi associati a tutto ciò: rischi legati alla sicurezza, ma anche rischi derivanti dall'uso dei dati e da una sottovalutazione delle conseguenze del particolare trattamento che si pone in essere. Rischi che possono incidere sulla vita fisica delle persone provocando danni rilevanti.

Il nuovo Regolamento Europeo sulla Protezione dei dati personali (GDPR) interviene direttamente nel rapporto tra innovazione digitale da un lato, diritti e libertà delle persone dall'altro, definendo nuovi obblighi per le aziende, come il *Data protection by design* e *Data protection impact assessment*.

Il Titolare del trattamento viene individuato dal Regolamento come il soggetto che meglio può valutare:

- come dare attuazione alla normativa nel proprio contesto operativo;
- responsabile (*accountable*) di questa valutazione e delle scelte conseguenti.

In questo contesto è necessario inserire la protezione dei dati personali tra i vincoli da considerare fin dai primi passi della progettazione di ogni nuovo servizio o prodotto, basato su dati personali e di cui tenere conto in ogni fase dello sviluppo del progetto.

Quando poi le caratteristiche del nuovo trattamento possono generare rischi particolari, anche in relazione all'uso di nuove tecnologie, scatta l'obbligo di un approfondimento mirato, un'analisi di impatto che può sfociare, se ritenuto necessario, nella consultazione preventiva dell'Autorità Garante per la protezione dei dati personali.

L'intero processo di innovazione rimane sotto il controllo del Titolare (il quale può anche avvalersi di un Responsabile per la protezione dei dati - DPO), che si assume in questo senso la piena responsabilità: ogni scelta deve essere documentata e comprovabile.

*Data protection by design* e *Data protection impact assessment* costituiscono quindi il filtro attraverso cui ogni innovazione deve passare: sono cioè lo strumento di governo della *digital transformation* per quanto attiene il rispetto delle libertà e dei diritti delle persone nell'era digitale. La loro valenza non riguarda tanto i trattamenti in essere, quanto tutta l'innovazione digitale.

Ma la sicurezza è solo uno dei principi applicabili al trattamento dei dati personali elencati nel GDPR. Occorre valutare il nuovo Regolamento nel suo complesso: gli attori primari responsabili di innescare queste procedure non sono dei professionisti della protezione dei dati personali (coloro che conoscono solo la normativa applicabile in materia), ma dei progettisti dell'innovazione.

Questi ultimi sono soggetti del tutto diversi, difficili da individuare a priori, con una formazione e una professionalità che raramente include competenze legali o una conoscenza approfondita della normativa.

Più che concentrarsi su complicate metodologie di *Data Protection by design*o di *Data Protection impact assessment*, è dunque essenziale lavorare per assicurarsi che:

- la consapevolezza della criticità del trattamento dei dati personali in ogni processo di innovazione diventi un elemento acquisito dalla cultura aziendale. Non è essenziale che tutti diventino esperti di *Data Protection* ma che tutti siano consapevoli del problema e sappiano/possano coinvolgere un supporto adeguato.
- le procedure da attivare per gestirle correttamente esistano e siano semplici, chiare, conosciute e facilmente raggiungibili e utilizzabili da chiunque.

In sintesi: è il rapporto fra azienda e innovazione a dover essere reso conforme al GDPR, con tutta la complessità che questo comporta. Non è un tema limitabile a chi si occupa di *compliance*, ma un tema che riguarda l'intera organizzazione.