Precisazioni e novità 2017 del WP29 sull'obbligatorietà o facoltatività della nomina del DPO

Date : 21 settembre 2017

Introduzione

A partire dal 25 maggio 2018 acquisirà efficacia in tutta Europa il Regolamento sulla protezione dei dati personali[1] fondato sul principio di responsabilizzazione del titolare (*accountability*) ed offre un orientamento in termini di *compliance* per la protezione dei dati in Europa. Al centro di questo nuovo quadro giuridico troviamo i responsabili della protezione dei dati (DPO) che avranno il compito di facilitare l'osservanza delle disposizioni del GDPR.

Tale figura è stata meglio esplicitata dal Gruppo di Lavoro "articolo 29" (WP29) nel provvedimento recante le Linee Guida del 13 dicembre 2017 WP 243 rev. 01, così come revisionato il 5 aprile 2017.

Vediamo quindi di fare un po' di chiarezza, proprio sulla base delle indicazioni esplicative contenute nelle Linee-Guida del WP29, al fine di determinare quando sia obbligatorio nominare un *Data Protection Officer*, o come risultante nella traduzione italiana, il Responsabile per la protezione dei dati; figura da non confondere con il Responsabile del trattamento del dato, già presente a partire dalla direttiva 95/46 che ha sempre affiancato in questi anni il Titolare del trattamento.

In base al Regolamento 2016/679/EU, alcuni titolari e responsabili del trattamento sono tenuti a nominare un DPO in via obbligatoria. Ciò vale per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche ovvero trattino su larga scala categorie particolari di dati personali (dati sensibili).

Anche ove il regolamento non imponga in modo specifico la designazione di un DPO, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "articolo 29" (WP29) incoraggia gli approcci di questo genere.

Le linee-guida del WPart. 29 gettano un po' di luce non solo sui requisiti che il DPO deve possedere, ma anche, aspetto che qui maggiormente rileva, sulle pertinenti disposizioni del

regolamento al fine di favorire l’osservanza della normativa da parte di titolari e responsabili del trattamento.

L’analisi parte proprio dall’obbligatorietà della nomina per determinati titolari del trattamento.

Ai sensi infatti dell’art. 37 Reg. 2016/679 la nomina di un DPO risulta obbligatoria in 3 casi definiti:

1. se il trattamento è svolto da un’autorità pubblica o da un organismo pubblico;
2. se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
3. se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Le attività che rendono obbligatoria la presenza del DPO all’interno dell’organizzazione sono quindi estremamente variegate e la lettera del Regolamento non le definisce altrimenti, lasciando ampi coni d’ombra che le Linee-Guida oggi in oggetto tendono a chiarire anche con esempi.

Gli interpreti si sono infatti fin da subito interrogati su cosa debba intendersi, ad esempio, per autorità o organismo pubblico, o in cosa consista il monitoraggio regolare e sistematico, o se la “larga scala” debba essere intesa come valore numerico in termini assoluti o percentuali.

Ma partiamo dall’inizio: chi sono i soggetti pubblici obbligati a nominare un DPO al proprio interno.

Autorità pubblica o organismo pubblico

Con tali sintagmi, “autorità pubblica” e “organismo pubblico”, il WP29 chiarisce che devono intendersi i soggetti definiti come tali dal diritto nazionale dello Stato in cui si verte.

La precisazione sembra per vero un po’ tautologica limitandosi ad affermare che sono enti pubblici, quelli definiti come tali dagli Stati. Al riguardo però sembra introdurre un’importante precisazione, allorquando afferma che sono autorità pubbliche o organismi pubblici non solo le autorità nazionali, regionali e locali ma, anche tutta una serie di altri organismi di diritto pubblico o comunque di soggetti che svolgano funzioni pubbliche o esercitino comunque pubblici poteri, come persone fisiche o giuridiche, di diritto pubblico o privato, in ambiti che variano a seconda delle disposizioni fissate nel diritto interno di ciascuno Stato membro: trasporti pubblici, forniture idriche ed elettriche, infrastrutture stradali, emittenti radiotelevisive pubbliche, istituti per l’edilizia pubblica o organismi di disciplina professionale.

In tutti questi casi la condizione di soggezione in cui versano gli interessati è infatti molto simile a quella in cui il trattamento è svolto da un’autorità pubblica o da un organismo pubblico. Si tratta di realtà in cui il singolo ha, in modo analogo alle autorità pubbliche, un margine esiguo o nullo rispetto alla possibilità di decidere se e come possano essere trattati i propri dati personali; pertanto, è verosimile che sia necessaria l’ulteriore tutela offerta dalla nomina di un DPO,

caldamente consigliata.

Le Attività principali

L’articolo 37, paragrafo 1, lettere b) e c) del Regolamento contiene un riferimento alle “attività principali del titolare del trattamento o del responsabile del trattamento”. Nel considerando n. 97 del Regolamento si afferma che le attività principali di un titolare del trattamento “riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria”.

Con “attività principali” si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento. Tuttavia, l’espressione “attività principali” non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare o dal responsabile.

Per esempio, l’attività principale di un ospedale consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente. Ne deriva che il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualsiasi ospedale, e che gli ospedali sono tenuti a nominare un DPO, come pure le cliniche private, che fanno del trattamento dei dati il proprio *core business*.

A titolo di ulteriore esemplificazione il WP29 cita il caso di un’impresa di sicurezza privata incaricata della sorveglianza di più centri commerciali e aree pubbliche. L’attività principale dell’impresa consiste nella sorveglianza, e questa, a sua volta, è legata in modo inscindibile al trattamento di dati personali. Ne consegue che anche l’impresa in oggetto deve nominare un DPO. D’altro canto, tutti gli organismi (pubblici e privati) svolgono determinate attività quali il pagamento delle retribuzioni al personale o la predisposizione di strutture standard di supporto informatico. Si tratta di esempi di funzioni di supporto necessarie ai fini dell’attività principale o dell’oggetto principale del singolo organismo, ma pur essendo necessarie o essenziali sono considerate solitamente accessorie e non vengono annoverate fra le attività principali, rendendo quindi facoltativa la nomina del DPO.

Larga scala

Anche il concetto di “larga scala” appare meritevole di chiarezza ed approfondimenti. Infatti, all’interno dell’articolo 37, paragrafo 1, lettere b) e c) del Regolamento, non si dà alcuna definizione di trattamento su larga scala, anche se il considerando 91 fornisce indicazioni in proposito. Il WP29 ammette che è impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità; ma, d’altra parte, ciò non preclude che, col tempo, sia possibile individuare alcuni standard utili a specificare in termini quantitativi cosa debba intendersi per “larga scala” con riguardo ad alcune tipologie di trattamento maggiormente comuni. Anche il WP29 intende contribuire alla definizione di questi standard pubblicando e mettendo a fattor comune esempi delle soglie applicabili per la nomina

di un RPD. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;

- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Alcuni esempi di trattamento su larga scala, afferma il WP29, 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 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.

Mentre, esempi di trattamento non su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Monitoraggio regolare e sistematico

Anche il "monitoraggio regolare e sistematico degli interessati" è un concetto piuttosto vago che non trova definizione all'interno del RGPD; tuttavia, il considerando 24 del Regolamento menziona il "monitoraggio del comportamento di detti interessati" ricomprendendovi senza dubbio tutte le forme di tracciamento e profilazione su Internet, anche per finalità di pubblicità comportamentale.

Occorre rilevare, però, che la nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente online, e che il tracciamento online va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati.

A giudizio del WP29 l'aggettivo "regolare" ha almeno uno dei seguenti significati:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico" ha almeno uno dei seguenti significati, a giudizio del WP29:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia

Le linee-guida contengono anche in questo caso al loro interno alcuni elenchi esemplificativi e non esaustivi per meglio far comprendere il concetto generali ed astratto contenuto nel Regolamento. Così va considerato monitoraggio regolare e sistematico: 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 valutazione 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.

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

È questo aspetto forse uno dei più chiari dell'art. 37 Reg. Pr., tant'è che anche il WP29 dedica a tale caso solo poche righe, riportando il testo di legge e affermando quindi che le disposizioni dell'art. 37, paragrafo 1, lettera c), riguardano il trattamento di categorie particolari di dati ai sensi dell'articolo 9 (dati sensibili) e di dati personali relativi a condanne penali e a reati.

Facoltatività della nomina

Fin qui si sono analizzati i casi di obbligatorietà di nomina di un DPO ai sensi del Regolamento 2016, ma il WP29 si spinge anche più in là, raccomandando a titolari e responsabili di documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se si applichi o meno l'obbligo di nomina di un DPO, così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti.

Tale analisi fa parte della documentazione da presentare, su richiesta, all'Autorità Garante per la protezione dei dati, in caso di verifiche, controlli ed ispezioni.

La documentazione sulla facoltatività e quindi sulla mancata adozione del DPO deve essere aggiornata ove necessario, per esempio se i titolari o i responsabili intraprendono nuove attività o forniscono nuovi servizi che potrebbero ricadere nel novero dei casi elencati all'art. 37,

paragrafo 1.

Nel caso in cui invece il titolare o il responsabile optino per la nomina di un DPO su base volontaria, troveranno applicazione tutti i requisiti di cui agli artt. 37-39 per quanto concerne la nomina stessa, lo status e i compiti del DPO, esattamente come nel caso di una nomina obbligatoria.

Nulla osta, precisa il WP29, a che un'azienda o un ente, quando non sia soggetta all'obbligo di designare un DPO e non intenda procedere a tale designazione su base volontaria, ricorra comunque a personale o consulenti esterni incaricati di incombenze relative alla protezione dei dati personali.

In tal caso è fondamentale però garantire che non vi siano ambiguità in termini di denominazione, *status* e compiti di queste figure; è dunque essenziale che in tutte le comunicazioni interne all'azienda e anche in quelle esterne (con l'autorità di controllo, gli interessati, i soggetti esterni in genere), queste figure o consulenti non siano indicati con la denominazione di Responsabile per la protezione dei dati (DPO), ma come semplici consulenti.

Queste considerazioni valgono anche per i Chief Privacy Officers (CPO) o altri professionisti in materia di privacy già operanti presso alcune aziende, che non sempre e non necessariamente si conformano ai requisiti fissati nel regolamento per quanto riguarda, per esempio, le risorse disponibili o la salvaguardia della loro indipendenza e che, in tal caso, non possono essere considerati e denominati "DPO". Si tenga presente che la designazione obbligatoria di un DPO può essere prevista anche in casi ulteriori in base alla legge nazionale o al diritto dell'UE. Occorrerà quindi aspettare e vedere se il legislatore italiano od europeo prevedrà ulteriori casi di estensione dell'obbligatorietà.

DPO condiviso

Un gruppo imprenditoriale può nominare un unico DPO a condizione che questi sia "facilmente raggiungibile da ciascuno stabilimento". Il concetto di raggiungibilità si riferisce ai compiti del DPO in quanto punto di contatto per gli interessati, l'autorità di controllo e isoggetti interni all'organismo o all'ente. Allo scopo di assicurare la raggiungibilità del DPO, interno o esterno, è importante garantire la disponibilità dei dati di contatto nei termini previsti dal GDPR. Il DPO deve essere in grado di comunicare con gli interessati in modo efficiente e di collaborare con le autorità di controllo interessate. Ciò è fondamentale al fine di garantire all'interessato la possibilità di contattare il DPO stesso.

Anche più autorità pubbliche o organismi pubblici possono designare un unico DPO in condivisione, tenuto conto della loro struttura organizzativa e dimensione. Poiché il DPO è chiamato a una molteplicità di funzioni, il titolare o il responsabile deve assicurarsi che un unico RPD, sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici.

[1] 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) (GU L 119, 4.5.2016). Il RGPD è rilevante ai fini del SEE e sarà applicabile una volta incorporato nell'Accordo relativo al SEE.

A cura di: **Elena Bassoli**