circolare
29 SETTEMBRE 2017

Studio
Arlati Ghislandi
CONSULENZA
DEL LAVORO E FISCALE

Milano, 29 settembre 2017

Oggetto

Responsabile della protezione dei dati – indicazioni del Garante della Privacy

Il Garante per la privacy italiano con propria recente newsletter ha fornito alcune indicazioni relativamente alla scelta del Responsabile della protezione dei dati (RPD), nuova figura introdotta dal Regolamento UE 2016/679.

Il contesto di riferimento

Il Legislatore Europeo ha promosso un Regolamento unico contenente alcune linee guida che gli stati membri debbono recepire, e se del caso normare, entro e non oltre il mese di maggio del prossimo anno. Tra le norme di rilievo sinergico del Regolamento, è prevista la nomina di un RPD che viene definita come obbligatoria in tre casi specifici:

a) quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico;
b) quando le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
c) quando il trattamento riguarda, sempre su larga scala, dati sensibili o relativi a condanne penali e reati.

Riteniamo opportuno con la presente analizzare alcuni termini con cui il Garante ha tradotto ufficialmente le linee guida del gruppo di lavoro europeo allo scopo di definire i soggetti tenuti alla nomina di tale figura nonché i compiti e le responsabilità connesse alla funzione del RPD.

> Per *"Attività principali"*

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.

Pur tuttavia l'espressione utilizzata 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. A titolo esemplificativo 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 RPD. O ancora il caso di un'impresa di sicurezza privata incaricata della sorveglianza di più centri commerciali e aree pubbliche in cui se è vero che l'attività principale dell'impresa consiste nella sorveglianza, e allo stesso tempo vero che questa sia a sua volta legata in modo inscindibile al trattamento di dati personali; con la necessaria conseguenza che anche l'impresa in oggetto deve nominare un RPD.

> Per *"Larga scala"*

Per far scattare l'obbligo di nomina di un RPD occorre che il trattamento dei dati personali avvenga su larga scala. Benché il regolamento non fornisca alcuna definizione in tal senso, sono da considerarsi trattamenti su larga scala quelli che hanno ad oggetto una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato.

Al fine di stabilire se un trattamento sia effettuato su larga scala occorre tenere conto dei seguenti fattori:
- 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.

> Per *"Monitoraggio regolare e sistematico"*
Anche tale concetto non trova definizione all'interno del RGPD.
Il "monitoraggio del comportamento di detti interessati" ricomprende senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale pur tuttavia sarebbe riduttivo isolarlo al solo ambiente on line il quale rimane solo uno dei possibili esempi di monitoraggio degli interessati.

L'aggettivo "regolare" fa riferimento ad un monitoraggio che assume 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.

Sarà da considerarsi invece "sistematico" il monitoraggio che ha almeno uno dei seguenti significati
- 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.

A titolo esemplificativo sono attività che possono configurare un monitoraggio regolare e sistematico di interessati quelle che riguardano: l'occuparsi del funzionamento di una rete di telecomunicazioni, la prestazione di servizi di telecomunicazioni, il reindirizzamento di messaggi di posta elettronica, l'attività di marketing basata sull'analisi dei dati raccolti, la profilazione e lo scoring per finalità di valutazione del rischio, i programmi di fidelizzazione, pubblicità comportamentale, il monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili, l'utilizzo di telecamere a circuito chiuso.

* * * * *

Da una prima disamina delle indicazioni di cui sopra emerge in modo chiaro che l'obbligo di nomina dell'RPD non sia legato al semplice trattamento del dato sensibile e che di conseguenza non tutti i Datori di Lavoro debbano procedere all'individuazione di una figura con tale mansione. L'obbligo non incorre infatti per il solo trattamento del dato ma assume rilevanza nella misura in cui il trattamento del dato sia o l'attività principale o sia ad essa legata in maniera inscindibile, e sia svolta in maniera strutturale, intesa come "servizio" di attività su larga scala.
Riteniamo al proposito che il Garante italiano debba nuovamente intervenire sull'argomento per non lasciare lasca un'identificazione funzionale che non può essere definita esauriente se esposta facendo ricorso a termini generici di carattere quantitativo.

* * * * *

I compiti del RPD
L'RPD ha fra gli altri il compito di sorvegliare l'osservanza del Regolamento Generale sulla protezione dei dati (Regolamento UE 2016/679) con particolare riferimento alle attività di raccolta di informazioni

per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile del trattamento dei dati.

In particolare il Responsabile della protezione dei dati dovrà:

a) informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) verificare l'attuazione e l'applicazione del Regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
c) fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;
d) fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;
e) fungere da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa.

L'RPD per tutte le questioni inerenti la protezione dei dati deve essere tempestivamente e adeguatamente coinvolto ed inoltre va sostenuto nell'esecuzione dei suoi compiti dal titolare e dal responsabile del trattamento che gli devono fornire tutte le risorse necessarie sia per svolgere il suo lavoro, sia per permettergli di mantenere aggiornata la sua conoscenza specialistica.

Nello svolgimento dei propri compiti l'RPD agirà in assoluta autonomia e indipendenza. Ciò vuol dire che non potrà ricevere alcuna istruzione circa l'esecuzione dei suoi compiti né potrà svolgere altre mansioni o compiti in conflitto di interessi con quelle proprie del RPD, essendo tenuto in ogni caso al segreto e alla riservatezza in ordine alle sue funzioni.

I requisiti del RPD

Il Responsabile della protezione dei dati è un professionista con conoscenze specialistiche della normativa e delle prassi in materia di protezione dati, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

1) possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
2) adempiere alle sue funzioni in piena indipendenza ed in assenza di conflitti di interesse;
3) operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio.

Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.
Pertanto, come chiarito dal Garante della Privacy, il RPD deve essere selezionato e scelto in base alle sue qualità professionali e in particolar modo sulla sua preparazione e conoscenza in ambito di trattamento dati, sia sul piano teorico che su quello pratico (normativa e prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento).
La scelta dovrà essere effettuata verificando la presenza di competenze ed esperienze specifiche.
Non sono richieste attestazioni formali sul possesso delle conoscenze o l'iscrizione ad appositi albi professionali.
L'Autorità chiarisce che nella selezione sarà opportuno privilegiare soggetti che possano dimostrare qualità professionali adeguate alla complessità del compito da svolgere, magari documentando le esperienze fatte, la partecipazione a master e corsi di studio/professionali.

Inoltre, il Garante precisa che la normativa attuale non prevede l'obbligo per i candidati di possedere attestati formali delle competenze professionali. Tali attestati, rilasciati anche all'esito di verifiche al termine di un ciclo di formazione, possono rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenza della disciplina ma, tuttavia, non equivalgono a una "abilitazione" allo svolgimento del ruolo di RPD.

Restando a disposizione per qualsiasi eventuale chiarimento, ci è gradita l'occasione per porgere i migliori saluti.

Daniela Ghislandi
Dottore Commercialista
Revisore contabile