diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

Chi è il responsabile della protezione dei dati?

Autore: Donato Sangiorgio
In: Diritto civile e commerciale

Il nuovo Regolamento Generale sulla Protezione dei Dati, (UE) 679/2016 conosciuto anche come "GDPR" con effetti diretti a partire dal 25 maggio 2018, è stato recepito dall'Italia col decreto legislativo n.101 del 10-08-2018, vigente dal 19 settembre 2018.

Il principio dell'accountability

La Commissione Europea, col GDPR, ha voluto consolidare la protezione dei dati personali dei cittadini dell'Unione Europea su un nuovo principio di **"responsabilizzazione" detto accountability.**

Il GDPR non ha dato una regola certa per definire il significato della responsabilizzazione, ma ha lasciato al Titolare del Trattamento la gestione dell'accountability, ma con la responsabilità di dimostrare al Garante, in fase di controllo, ciò che ha fatto.

La figura e la nomina del RPD

Insieme a questo nuovo principio, nel GDPR e poi nella disposizione di legge italiana, è stato inserito il **Responsabile della Protezione dei Dati (RPD),** interpellato ad agevolare l'applicazione del GDPR, figura obbligatoria nella P.A. mentre nelle strutture private solo dove è previsto.

L'RPD è nominato dal titolare del trattamento o/e dal responsabile del trattamento e la sua nomina è obbligatoria in tre casi:

1) amministrazioni, enti pubblici e autorità giudiziarie nell'esercizio delle loro funzioni;

2) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su **larga scala;**

3) tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Attenzione però, l'art. 32 della direttiva (UE) 680 del 2016 al comma 1 così recita "…Gli Stati membri

Diritto & Diritti ISSN 1127-8579

possono esentare le autorità giurisdizionali e le altre autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali da tale obbligo…".

L'RGDP inserisce un'altra condizione per rendere obbligatoria la nomina dell'RPD, bisogna che il trattamento dei dati personali avvenga su **larga scala**. Non è ben definita la definizione di larga scala nel regolamento, anche dopo aver letto il considerando 91. Ecco che, il Gruppo di lavoro articolo 29 per la protezione dei dati, designa una definizione più tecnica di cosa si intende per larga scala, elencando esempi per la nomina del RPD:

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

Alcuni esempi di trattamento su larga scala sono i seguenti:

1. trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
2. trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
3. 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;
4. trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
5. trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
6. trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Alcuni esempi di trattamento non su larga scala sono i seguenti:

Diritto & Diritti ISSN 1127-8579

1. trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;

2. trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

I requisiti dell'RPD:

1. 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.

All'art. 37 del regolamento non si leggono requisiti precisi a carico del RPD, ma indica semplicemente che **deve essere in possesso di qualifiche professionali, presumendo partecipazione a master e corsi di studio/professionali, per raggiungere una adeguata conoscenza;**

2. adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. In linea di principio, ciò significa che il RPD non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali;

3. operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio (RPD esterno).

Vedi:"General Data Protection Regulation"

I compiti dell'RDP:

a) sorvegliare l'osservanza del regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;

b) collaborare con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);

c) informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi

Diritto & Diritti ISSN 1127-8579

ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;

d) cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;

e) supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento.

L' RPD **non deve ricevere alcuna istruzione circa l'esecuzione dei suoi compiti,** deve poter agire in maniera indipendente, deve riferire sempre al vertice gerarchico garantendo che quest'ultimo venga a conoscenza delle indicazioni e delle raccomandazioni fornite dal RPD nell'esercizio delle funzioni di informazione e consulenza a favore del titolare o del responsabile.

Se l'incarico di RPD viene affidato ad un dipendente interno, è utile investire a tale figura un dirigente o un funzionario di alta professionalità, in grado di svolgere **autonomamente** le proprie funzioni.

Per tale la nomina di RPD interno, occorre un apposito atto di designazione a Responsabile per la protezione dei dati, se invece è esterno all'ente, la designazione verrà svolta con contratto di servizi, motivando la nomina. Il nominativo di RPD, scelto di nuova nomina o in variazione del nominativo, dovrà essere comunicato al Garante, per agevolare i contatti con l'Autorità, indicarlo nella informativa fornita agli interessati, pubblicare il nominativo (anche se non è obbligatorio inserire il nominativo del RPD) sul sito web nella sezione amministrazione trasparente, nella sezione privacy, comunicare il nominativo agli interessati in caso di violazione dei dati personali.

Volume consigliato

https://www.diritto.it/chi-e-il-responsabile-della-protezione-dei-dati/

Diritto & Diritti ISSN 1127-8579