TeLex Anie
NOVITÀ LEGISLATIVE E GIURISPRUDENZIALI
Estratto
N. 6 Anno XXII
Giugno 2017

PRIVACY

IL DATA PROTECTION OFFICER

Quadro normativo. Il Regolamento UE 2016/679 tratta la figura del Data Protection Officer agli artt. 37, 38 e 39. La figura è introdotta dal 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 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».

Il ruolo del Data protection officer e origini storiche. Quello del data protection officer è un ruolo che ricorda la figura professionale del Chief Privacy Officer. Quest'ultima è una figura professionale, che, nata negli Stati Uniti, si caratterizza per le competenze giuridiche ed informatiche e a cui compete la responsabilità di osservare, valutare e organizzare la gestione del trattamento di dati personali (e, dunque, la loro protezione) all'interno di una organizzazione, affinché questi siano trattatati in modo lecito e pertinente, nel rispetto delle normative vigenti.
Non si tratta di una novità assoluta, in quanto la sua presenza, in base all'art. 18 della Direttiva 95/46/Ce, è già obbligatoria in diverse nazioni europee (es. Germania, Grecia, Ungheria, Slovacchia), mentre è facoltativa in altre, come la Francia.
Storicamente in Italia, il Garante si è occupato di questa figura già nel 2012, come emerge dalla relazione annuale al Parlamento: «*Un ruolo positivo è sicuramente giocato dalle figure di responsabili privacy, oramai piuttosto diffuse, che, coordinando e indirizzando l'azione degli uffici periferici, assicurano una più puntuale e attenta applicazione della legge. In una qualche misura, dall'esperienza di queste nuove figure professionali viene quasi anticipata la funzione del privacy officer, ben conosciuta in altri ordinamenti e recentemente inserita nelle bozze del nuovo regolamento comunitario in materia di protezione dei dati personali.*».
Anche nelle Linee Guida sul Dossier Sanitario Elettronico del 04 giugno 2015, il Garante ha auspicato che i Titolari del trattamento individuino al loro interno una figura di responsabile della protezione dei dati: " il Garante auspica che i titolari del trattamento individuino al loro interno una figura di responsabile della protezione dei dati che svolga il ruolo di referente con il Garante (c.d. DPO- data protection officer), anche in relazione ai casi di data breach . . ."

Quando il DPO è obbligatorio. La nuova disciplina europea stabilisce che la designazione del D.P.O. sia obbligatoria quando ricorrano alternativamente i seguenti presupposti:

- (a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, ad eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali; o
- (b) le attività principali del Titolare (Data Controller) o del Responsabile (Data Processor) consistono in trattamenti che, richiedono il monitoraggio regolare e sistematico di interessati su larga scala; o
- (c) le attività principali del Titolare (Data Controller) o del Responsabile (Data Processor) consistono nel trattamento su larga scala di categorie particolare di dati (art. 9) o di dati personali relativi a condanne penali e reati (art. 10);

Con le linee guida adottate il 13 dicembre 2016 (WP 243) il Gruppo di lavoro dei garanti europei (c.d. "Articolo 29") ha fornito indicazioni interpretative in

merito ai concetti di attività principale, larga scala e monitoraggio regolare e sistematico.

I compiti del DPO. Ai sensi dell'articolo 38 del nuovo regolamento il Titolare e il Responsabile assicurano che il data protection officer sia *tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.*
I compiti di un data protection officer possono essere esemplificativamente riassunti come segue:

1) sorvegliare la corretta applicazione della normativa sulla protezione dei dati;
2) effettuare privacy impact assessment di progetti;
3) verificare la corretta applicazione della protezione dei dati sin dalla progettazione di applicativi (c.d. privacy by design), controllando che gli stessi abbiano impostazioni privacy predefinite (c.d. privacy by default);
4) effettuare audit;
5) collaborare con le Autorità competenti (prima fra tutte l'Autorità Garante per la protezione dei dati personali);
6) controllare che le violazioni dei dati personali siano documentate, notificate e comunicate (c.d. Data Breach Notification).

L'articolo 38, secondo paragrafo del regolamento obbliga il titolare o il responsabile a sostenere il data protection officer *fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.*
Infatti, in base all'articolo 37, paragrafo 5, il DPO *è 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'articolo 39.*

Le qualità professionali del DPO. Come precisato dai garanti europei il livello di conoscenza specialistica richiesto dalla normativa non trova una definizione tassativa; piuttosto, deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento. Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il DPO avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto. Occorre anche distinguere in base all'esistenza di trasferimenti sistematici ovvero occasionali di dati personali al di fuori dell'Unione europea. Ne consegue la necessità di una particolare attenzione nella scelta del DPO, in cui si tenga adeguatamente conto delle problematiche in materia di protezione dei dati con cui il singolo titolare deve confrontarsi.

Caso pratico. Un'impresa di sicurezza privata che svolge attività di sorveglianza nei confronti di alcuni centri commerciali e aree pubbliche è obbligata a nominare la figura del data protection officer ?
Come osservato dai Garanti Europei 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.
Conclusioni. Il Regolamento UE 2016/679 riconosce nel Data Protection Officer uno degli elementi-chiave all'interno del nuovo sistema di *governance* dei dati, che alla luce dell'altro fondamentale principio introdotto dal Regolamento, quello dell'acountability, fanno sì che soggetti privati e pubblici non potranno limitarsi agli adempimenti minimi, ma dovranno dimostrare con evidenze oggettive di avere implementato idonee misure a tutela della sicurezza dei trattamenti.

Avv. Marco Soffientini
Studio Legale Rosadi Soffientini Associati

Proprietario ed editore:
Federazione ANIE
Viale Lancetti 43, 20158, MI
Telefono (02) 3264.1
Direttore Responsabile
Maria Antonietta Portaluri
Registrazione del Tribunale
di Milano al n° 116 del
19/2/1996

***Te*Lex Anie**

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE
CONFINDUSTRIA

Pubblicazione a cura di:
Servizio Centrale Legale
Viale Lancetti 43, 20158, MI
Telefono (02) 3264.246
e-mail legale@anie.it
Diffusione via web www.anie.it

Mini Master ANIE sulla Privacy: partecipa