Giancarlo Butti,
Maria Roberta Perugini

GDPR
La privacy nella pratica quotidiana

Tutte le domande a cui un DPO deve sapere rispondere

MANAGEMENT

FrancoAngeli

TOOLS

Indice

Introduzione

L'idea di questa pubblicazione nasce dall'esperienza maturata non solo nel corso dell'attività professionale ma anche in occasione dei numerosi corsi e master che ci hanno visti come docenti in questi anni.

Molto spesso, nonostante il livello di preparazione degli allievi fosse alto ed il loro ruolo rilevante (molti DPO e consulenti), riscontravamo aree grigie in merito a elementi basilari relativi alla conoscenza della normativa, foriere di rilevanti conseguenze.

Una non corretta individuazione di quali siano i dati personali trattati dalla propria organizzazione o delle categorie di interessati può fare sì che il perimetro di applicazione di tutte le misure messe in atto per il rispetto della normativa privacy sia errato, escludendo dalla tutela fasce più o meno rilevanti di persone fisiche o di dati personali.

Le conseguenze sono il rischio di sanzioni o di risarcimento danni ai sensi dell'art. 82 del GDPR, oltre agli effetti negativi indiretti connessi alla perdita d'immagine dell'organizzazione Titolare.

A questo esempio se ne possono aggiungere molti altri, derivanti da un approccio troppo spesso meccanicistico e scolastico nei confronti di una normativa eccezionalmente complessa, articolata e ricca di interazioni sia interne (intendendo con tale termine il legame, spesso non evidente, fra i vari adempimenti normativi) sia esterne.

A ciò spesso contribuisce la scarsa conoscenza della normativa, appresa più per "sentito dire", tramite corsi e pubblicazioni, piuttosto che dalla sua lettura diretta, nonché una analisi troppo superficiale.

Ecco quindi che credenze diffuse si diffondono e mistificano la norma.

Molti confondono la DPIA con l'analisi dei rischi, o scambiano i diritti e libertà delle persone fisiche (come recita la normativa) con quelli dei soli interessati.

Da qui la necessità di fare chiarezza e il motivo per cui, in luogo di semplici interpretazioni, è importante ripartire dal testo effettivo della normativa, troppo spesso ignorato.

Il libro vuole essere uno strumento realmente operativo, ma anche rigoroso nei contenuti. Per tale motivo, in luogo di una serie di modelli e modulistica autoprodotta sono riportate nelle appendici (disponbili on line) i riferimenti a modulistica e strumenti "ufficiali", in quanto proposti da Autorità Garanti.

Infine, pur volendo essere il più possibile oggettivo, il testo riporta ovviamente le opinioni degli autori[1] e come tale deve essere considerato.

Lo spazio necessariamente limitato ci ha costretto a selezionare alcuni argomenti e temi tralasciandone altri, e il taglio strettamente operativo non ci ha consentito di sviluppare verticalmente alcune questioni di cui abbiamo fornito direttamente le conclusioni: ove possibile abbiamo suggerito in nota fonti utili per approfondire.

Segnaliamo infine che nel nostro blog professionale **www.mrperugini.it**, oltre a studi e documenti utili, è presente una sezione dedicata a questo libro in cui pubblicheremo note e articoli di approfondimento e aggiornamento dei temi qui trattati e dove affronteremo altre problematiche di interesse per i DPO.

In particolare, contestualmente alla pubblicazione del testo saranno disponibili una serie di Appendici.

Per la realizzazione del testo sono stati utilizzati contributi che negli anni sono stati pubblicati in particolare sul blog collettivo blog.europrivacy.info e sulle riviste online Cybersecurity360 (cybersecurity360.it), Cybersecurity Trends (www.cybertrends.it/rivista/), Toolnews (itware.com).

Al riguardo un ringraziamento va ad Alessandro Longo, Alessandro Giacchino, Elena Agresti.

Alcuni spunti derivano inoltre dalla nostra precedente pubblicazione del 2019 per FrancoAngeli "Audit e GDPR - Manuale per le attività di verifica e sorveglianza del titolare e del DPO (Data Protection Officer)".

Convenzioni utilizzate nel testo

All'interno di questo documento si utilizzeranno le seguenti convenzioni.
Il termine "soluzioni ufficiali" indica che tali soluzioni sono realizzate:

- da autorità garanti degli Stati membri;
- dall'autorità garante europea – edps.europa.eu;
- dal Comitato europeo per la protezione dei dati (ex WP29) – edpb.europa.eu/edpb_it;
- da ENISA – www.enisa.europa.eu/;

il termine "normativa" può comprendere anche le "soluzioni ufficiali"; il termine "soluzioni autorevoli" indica che sono realizzate da enti di normazione, quali:

1. Opinioni che derivano da oltre 20 anni di "pratica" nel campo della protezione dei dati personali.

- ISO – www.iso.gov;
- NIST – www.nist.gov.

Si citeranno inoltre:

- Autorità Garante (Autorità Garante per la protezione dei dati personali italiana) – www.garanteprivacy.it/;
- CNIL – Commission Nationale de l'Informatique et des Libertés (Autorità di controllo francese) – www.cnil.fr;
- AEPD (Autorità di controllo spagnola) – www.aepd.es;
- ICO Information Commissioner's Office (Autorità di controllo inglese) – ico.org.uk;
- OECD (Organisation for Economic Co-operation and Development) – www.oecd.org/.

I termini "titolare" e "responsabile", quando indicano i relativi ruoli previsti dagli artt. 24 e 28 del GDPR saranno scritti, a soli fini identificativi, come Titolare e Responsabile.

I termini "azienda", "organizzazione", "ente" vengono spesso utilizzati per indicare genericamente un ente che effettua un trattamento di dati personali.

Il termine "privacy" viene utilizzato generalmente per intendere la complessiva normativa applicabile in materia di protezione dei dati personali.