filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

GDPR, un approccio basato sul rischio. Riflessioni e una soluzione utile

14 Maggio 2019
Marco Dettori

Indice:

1. Premessa

Il Regolamento (UE) 679/2016 ("GDPR") ha apportato significative modifiche alla disciplina sul trattamento dei dati personali, generando uno **scalpore mediatico di notevoli proporzioni**, forse, anche, per merito (o colpa) degli importi delle sanzioni applicabili.

In ambito commerciale e aziendale, la bufera mediatica ha avuto, da un lato, **l'effetto di generare la "corsa alla conformità"** delle aziende italiane per evitare sanzioni da 10 o 20 milioni di euro, dall'altro, **l'effetto di rendere più consapevoli imprenditori e aziende** dell'esistenza di tale normativa, spesso trascurata.

Nonostante il giustificato timore suscitato dalle sanzioni, in realtà, l'approccio e la "filosofia" del GDPR – se letti in chiave positiva – non sono più stringenti di quanto non lo fosse la precedente normativa, anzi, **si rileva una maggiore apertura in favore della libera circolazione dei dati personali** all'interno dell'Unione Europea e una **maggiore autonomia per i titolari del trattamento** nell'adempimento degli obblighi.

> **A livello nazionale, molti titolari del trattamento – soprattutto PMI – fanno fatica a scorgere nell'adeguamento al GDPR un'opportunità di crescita e di investimento per le proprie aziende, percependolo invece come un gravoso adempimento obbligatorio, statico e formale.**

Tra le barriere che impediscono ai titolari del trattamento di avere una visione "positiva", va rilevata senz'altro l'**elevata complessità della disciplina, dal punto di vista terminologico, di contenuto e di applicabilità operativa**.

Per tali ragioni, **un titolare del trattamento che non ha mai curato l'aspetto *data protection* nell'ambito della propria attività**, si trova necessariamente ad affrontare un costo notevole per adeguare la propria azienda/realtà ad una normativa che **risulta praticamente impossibile applicare correttamente per i "non addetti ai lavori"**.

> **In quest'ottica risulta fondamentale il ruolo (e l'onestà professionale) degli operatori della materia, quali consulenti, *Data Protection Officer*, società di consulenza, *data manager*, ecc., che assumono l'importante compito di "tradurre" il linguaggio del GDPR e trasmetterne i principi cardine ai titolari del trattamento, in modo tale da ingenerare in loro quella coscienza e sensibilità (oltre alla consapevolezza dei relativi obblighi) che sta alla base del principio di responsabilizzazione (cosiddetta "*accountability*") sul quale è costruito l'intero impianto del GDPR.**

Fatta questa premessa, con la rubrica "Il dato è tratto" ci si propone di contribuire, per quanto possibile, al processo di sensibilizzazione e divulgazione di tale principio, al centro di tutto il trattamento dei dati personali, con un *focus* particolare all'ambito commerciale e aziendale.

2. L'approccio basato sul rischio: il comune denominatore di principi e obblighi del GDPR

L'approccio basato sul rischio permea l'intera logica applicativa del GDPR e porta il titolare **a dover considerare "rischioso" per l'interessato qualsiasi trattamento di dati personali** al quale sia applicabile il GDPR.

Per tale ragione, **la consapevolezza** che chi tratta dati personali in qualità di titolare del trattamento **espone l'interessato a potenziali rischi, è il punto di partenza** per un corretto recepimento dei principi fondanti del GDPR. Alcuni di tali principi, quali l'*accountability* e la privacy *by design* e *by default*, non fanno altro che guidare i titolari del trattamento verso l'adozione di misure e cautele che consentono di trattare i dati personali limitando il più possibile i rischi per gli interessati.

L'approccio basato sul rischio può tradursi come l'**analisi preventiva del contesto del trattamento, del grado di probabilità e di gravità dei potenziali rischi** ai quali è esposto l'interessato e, di conseguenza, la **predisposizione di piani di azione** volti a limitare il verificarsi degli eventi a rischio.

> **Si tratta di un processo di autovalutazione, all'esito del quale il titolare deve adottare le cautele e le misure che risultino (e che ritiene) più idonee a tutelare e proteggere gli interessati e i relativi dati personali.**

Il principio di *accountability*, insieme all'approccio basato sul rischio, determina **il superamento del concetto di misure "minime di sicurezza" della precedente disciplina**, colpevole di aver ingenerato nei titolari la percezione errata che la conformità alla normativa e la tutela dei dati personali potesse essere conseguita mediante **adempimenti meramente formali**, scollegati dallo specifico contesto di trattamento e **replicati con modelli documentali standard** per realtà eterogenee e diverse tra di loro.

3. La valutazione di impatto come obbligo e come *best practice*

Sulla base dei citati principi e dell'approccio basato sul rischio, il GDPR ha previsto **un adempimento obbligatorio, la cosiddetta valutazione di impatto** (*Data Protection Impact Assessment*, "DPIA"), finalizzato a tutelare i casi in cui **i rischi ai quali si espone l'interessato siano particolarmente elevati** e mettano in pericolo i diritti e le libertà delle persone fisiche.

Senza entrare nel merito degli aspetti interpretativi e applicativi della relativa norma (articolo 35 del GDPR), già ampiamente trattati in più occasioni e da più fonti, si rileva **l'importanza della valutazione di impatto e i suoi benefici**, per i titolari del trattamento, in termini di **conformità e di adeguatezza** nella gestione del rischio.

> **La predisposizione di una valutazione di impatto, che segua la procedura e i contenuti esposti dallo stesso GDPR, è stata fortemente auspicata dal Gruppo di Lavoro *ex* articolo 29 e dal Garante Privacy, anche fuori dai casi in cui è obbligatoria.**

Una scelta in tal senso, da parte di un titolare del trattamento non obbligato, **figurerebbe senz'altro come l'adozione di una *best practice***, in perfetta sintonia con l'applicazione del principio di *accountability* e dell'approccio basato sul rischio.

4. Un *software* consigliato per la predisposizione della DPIA

Con la nota del 1 giugno 2018 "*Un software per la valutazione di impatto*", il Garante Privacy ha segnalato la versione italiana di un *software* gratuito, predisposto dalla CNIL (il garante privacy francese), mediante il quale **è possibile effettuare una valutazione di impatto** dei trattamenti desiderati.

> **Il link al sito dal quale è possibile scaricare il *software* e consultare le istruzioni per l'installazione è il seguente: https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.**

Il *software* offre un **ausilio metodologico** ai titolari del trattamento, soprattutto per le PMI, senza costituire un modello assoluto di conformità alla normativa.

La **procedura di valutazione proposta con il *software* è scandita in fasi**, sostanzialmente corrispondenti ai passaggi previsti dalla norma, e ha la funzione di orientare il titolare nell'analisi e nella valutazione di:

- **contesto dei trattamenti**,
- **esposizione ai relativi rischi**,
- **misure di sicurezza** adottate,
- **mappatura globale dei rischi** e
- **piani di azione** predisposti per mitigare tali rischi.

Il *software* prevede **l'intervento di tre figure distinte** nell'ambito della valutazione, alle quali sono attribuiti funzioni e compiti differenti. È prevista:

- la redazione da parte di un "**autore**";
- la revisione/valutazione con commenti da parte di un "**revisore**";
- la validazione da parte di un "**validatore**".

La redazione della valutazione deve essere completa, altrimenti il revisore non potrà effettuare la propria attività di controllo e revisione. Allo stesso modo, la valutazione potrà essere validata solo all'esito del completamento dell'attività di revisione.

Nel caso in cui il titolare abbia nominato **un Data Protection Officer**, nell'ambito della procedura, il *software* **consente di raccogliere il relativo parere** prima della validazione finale.

Nonostante la corretta indicazione del Garante in merito alla "non universalità" del *software* rispetto a qualsiasi trattamento, **tale strumento rappresenta un valido ausilio e una misura organizzativa utile** – sia per i titolari del trattamento più consapevoli che per gli addetti ai lavori – per la gestione generale del rischio "fisiologico" derivante dal trattamento di dati personali.

Nell'ambito dell'attività di consulenza svolta verso alcuni dei nostri clienti, abbiamo utilizzato il *software* in oggetto e l'abbiamo trovato utile per le seguenti ragioni:

tecnico-informatiche

- il fatto che sia rilasciato con codice *open source*, con possibilità di adattamento a diversi ambienti informatici;
- versione *portable* che consente l'utilizzo sul dispositivo senza installazione in locale;
- buona usabilità e comprensione;
- possibilità di stampare la valutazione d'impatto;

di contenuto

- sezioni didattiche e esplicative chiare e complete, poste a margine dell'interfaccia in modo tale da guidare l'utente passo per passo;
- accurato elenco di misure di sicurezza tecniche e organizzative esplicate;
- scheda grafica finale che espone il rapporto tra le misure adottate e le categorie di rischio.

Letture consigliate:

Linee Guida sulla Valutazione di impatto del Gruppo di Lavoro *ex* articolo 29:

- https://ec.europa.eu/newsroom/article29/itemdetail.cfm?item_id=611236

Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018 [9058979] del Garante Privacy:

- https://www.garanteprivacy.it/web/guest/home/docweb//docweb-display/docweb/9058979

Nota del Garante Privacy "*Un software per la valutazione di impatto*":

- https://www.garanteprivacy.it/web/guest/home/docweb//docweb-display/docweb/8581268

"*Valutazione d'impatto - Garante per la protezione dei dati personali: gli specifici casi in cui è obbligatorio il Dpia*", Articolo pubblicato su Filodiritto dalla Dottoressa Carolina Sartoni:

- https://www.filodiritto.com/news/2018/valutazionedimpatto-garante-per-la-protezione-dei-dati-personali-gli-specifici-casi-in-cui-obbligatorio-il-dpia.html

TAG: *GDPR, privacy, Misure di sicurezza, dati personali, valutazione di impatto*
