Bologna

15 maggio 2018

"La gestione del rischio privacy e l'impatto sull'organizzazione aziendale"

Studio Legale Piccaglia

La gestione del rischio privacy

L'analisi del rischio *privacy* ha un ruolo fondamentale nel Regolamento Europeo per la *Data Protection.*

E' lo strumento per dimostrare l'adeguatezza delle misure implementate a tutela dei dati trattati.

Introduce l'approccio basato sul **rischio** che si traduce in una serie di disposizioni che tendono a promuovere approcci basati sulla prevenzione di possibili problematiche e sulla riduzione degli oneri burocratici.

Definizione

Uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità per i diritti e le libertà

(linee Guida del gruppo di lavoro articolo 29 wp)

Considerando 75

*I r**ischi** per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, **possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale**, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.*

Cos'è il rischio privacy

- il rischio di non conformità;
- il rischio di non adempiere agli obblighi;
- il rischio di commettere o di non impedire di commettere violazione di dati personali, ossia la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione non autorizzata o accesso a dati personali trasmessi, conservati o comunque trattati.

Rischio inerente il trattamento

Rischio di impatti negativi su libertà e diritti degli interessati che devono essere analizzati attraverso un apposito processo di valutazione, tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative che il titolare ritiene di dovere adottare per mitigare i rischi.

In particolare la sicurezza del trattamento riguarda la:

- disponibilità (distruzione, indisponibilità, perdita);
- integrità (alterazione);
- riservatezza (divulgazione, accesso).

Novità

- valutazione d'impatto sulla protezione dei dati;
- diritto alla portabilità;
- *data breach*;
- registri delle attività di trattamento;
- certificazione;
- consultazione preventiva.

Contenuto minimo valutazione d'impatto

- descrizione di trattamenti, finalità e interesse legittimo perseguito;
- valutazione della necessità e proporzionalità dei trattamenti rispetto alle finalità;
- valutazione dei rischi per i diritti degli interessati;
- misure previste contro questi rischi.

Accountability

Il GDPR non indica puntualmente le linee guida per proteggere le informazioni, ma chiede a titolari e responsabili l'adozione di *comportamenti proattivi* e non reattivi al fine da dimostrare la concreta adozione del regolamento.

L'*accountability*:

- **trasparenza:** accessibilità alle informazioni;
- **rendiconto**: dare prova dell'adozione di misure tecniche, giuridiche e organizzative (che devono essere riesaminate e aggiornate se necessario), anche attraverso modelli *ex* D.Lgs 231/2001;
- **responsabilità**: capacità di fare rispettare norme e regole di comportamento.

Art. 5 comma 2 Regolamento:

"il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo (responsabilizzazione) …".

E' quindi necessario, per dimostrare l'*accountability* richiesta dal Regolamento, **seguire un percorso logico, che dimostri come si sono protette le informazioni gestite e quali rischi corrono gli interessati che autorizzano a trattare i loro dati**.

Modello

Per quanto riguarda le novità normative introdotte in tema di privacy, l'entrata in vigore del Regolamento comporterà un'integrazione dei modelli organizzativi e dei *compliance program*, un aggiornamento del sistema dei controlli interni e nella gestione dei *data breach,* oltre che un'integrazione dei ruoli coinvolti nel processo di *privacy compliance*: DPO, *Audit, Compliance*, Ufficio Legale e OdV.

Approccio basato sul rischio e misure di *accountability* di titolari e responsabili

E' dunque affidato ai titolari il compito di decidere autonomamente:

- modalità
- garanzie
- limiti

del trattamento dei dati personali nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento …

Tra cui:

- l'applicazione dei principi di *data protection by design* e *by default* (art. 25 del Regolamento), ossia la necessità di configurare il trattamento prevedendo, sin dall'inizio, garanzie indispensabili per soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per diritti e libertà degli interessati;
- obbligo di condurre una valutazione d'impatto prima di procedere a un nuovo trattamento, seguita eventualmente dalla consultazione dell'autorità di controllo qualora il titolare non ritenga sufficienti le misure di mitigazione del rischio a lui note o disponibili;
- l'introduzione della figura del DPO;
- la notifica di eventuali violazioni di dati personali (*data breach*) ad Autorità ed interessati;

Misure per la gestione del rischio

- **Organizzative**: ruoli, *governance*, istruzioni, formazione, procedure, *audit*;
- **Tecnologiche**: *policy* di sicurezza logiche e fisiche, aggiornamenti, *software*, tracciabilità delle operazioni.

Art. 24 Regolamento - Responsabilità del titolare del trattamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, ***il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.*** *Dette misure sono riesaminate e aggiornate qualora necessario …".*

Cosa dovrebbe fare un'Azienda?

- dotarsi di un modello di organizzazione, gestione e controllo del rischio *privacy;*
- responsabilizzare, formare e sensibilizzare le risorse sul rispetto della normativa e sui rischi;
- predisporre procedure tese ad evitare il rischio *privacy;*
- predisporre un organigramma *privacy* ed impostare una corretta distribuzione di compiti e responsabilità nel trattamento e vigilare.

Impatto sull'Azienda

- regole di organizzazione per il corretto trattamento (consenso);
- sanzioni commisurate al fatturato;
- meccanismi di tracciabilità che impongono la distribuzione delle responsabilità;
- dovere di documentazione ed informazione.

La gestione del rischio privacy

Art. 24 comma 3 Regolamento:

"*L'adesione ai codici di condotta di cui all'articolo 40* (Codici di Condotta) *o a un meccanismo di certificazione di cui all'articolo 42* (Certificazione) *può essere utilizzata* ***come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento*** *…".*

Bologna

15 maggio 2018

"reati informatici previsti dal codice penale e la responsabilità amministrativa degli enti"

Studio Legale Piccaglia

Con la Legge 25 ottobre 2017, n. 163 il Parlamento ha incaricato il Governo di:

a) abrogare espressamente le disposizioni del D.Lgs. 196/2003 che siano in contrasto o incompatibili con la nuova disciplina europea;

b) modificare le norme del c.d codice privacy al fine di dare puntuale attuazione alle disposizioni del Regolamento;

c) coordinare la normativa italiana in ambito di protezione dei dati personali con quanto previsto dal GDPR;

d) adottare, ove necessario, provvedimenti specifici, nel rispetto degli interventi del Garante in materia;

e) adeguare l'apparato sanzionatorio previsto dalla normativa italiana al GDPR, prevedendo sanzioni penali e amministrative adeguate alle violazioni

Sanzioni

- Le sanzioni per l'inosservanza della normativa *data protection* non si limiteranno alle sanzioni amministrative pecuniarie (€ 20.000.000 o per le imprese fino al 4% del fatturato mondiale totale annuo, *ex* art. 83 Regolamento);
- Le sanzioni che, secondo quanto recentemente ricordato dal Garante, saranno operative dal 25 maggio, non subiranno proroghe o sospensioni temporanee …
- Alle sanzioni pecuniarie sono da aggiungere gli illeciti previsti nel codice penale che sono stati ricompresi nell'elenco dei reati presupposto, ai sensi del D.Lgs 231/2001 (***art. 24 bis delitti informatici e trattamenti illecito dei dati***), ad esempio: accesso abusivo a sistemi informatici (art. 615 *bis*), appropriazione e diffusione abusiva di codici di accesso (art. 615 *quater*), danneggiamento di informazioni, dati, programmi informatici (art. 640 *bis*) e dei sistemi informativi (art. 640 *quater*).

Sanzioni

Le sanzioni penali saranno stabilite con decreto legislativo di coordinamento (con la normativa privacy in vigore) non ancora esistente che dovrà essere introdotta entro la data del 21 maggio prossimo, qualora si accertasse il trattamento illecito dei dati, la falsità nelle dichiarazioni e notificazioni al Garante oltre che l'inosservanza di misure di sicurezza e dei provvedimenti del garante

Art. 24-bis. *Delitti informatici e trattamento illecito di dati*

1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.

2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.

3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.

4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

sanzione pecuniaria da cento a cinquecento quote

Art. 615-ter c.p. - Accesso abusivo ad un sistema informatico o telematico

Art. 617-quater c.p. -Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche

Art. 617-quinquies c.p. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

Art. 635-bis c.p. Danneggiamento di informazioni, dati e programmi informatici

Art. 635-ter c.p. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

Art. 635-quater c.p. - Danneggiamento di sistemi informatici o telematici

Art. 635-quinquies c.p. -Danneggiamento di sistemi informatici o telematici di pubblica utilità

sanzione pecuniaria sino a trecento quote

Art. 615-quater c.p. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Art 615 quinquies c.p. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

sanzione pecuniaria sino a quattrocento quote

Art. 640 quinquies c.p. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

Studio Legale Piccaglia

le slide sono disponibili sul sito:
www.studiopiccaglia.com