COLIN
CONSULENTE LEGALE INFORMATICO

Qual è l'impatto dell'adeguamento GDPR sulle misure per la sicurezza nelle aziende italiane?

Avv. Valentina Frediani

Founder e CEO Colin & Partners

Milano

Cybersecurity Summit

7 Giugno 2017

OCSE a imprese e Governi: considerare la sicurezza informatica un rischio economico

Il rischio per la sicurezza digitale dovrebbe essere considerato un **problema di ordine economico e non solo tecnologico, e dovrebbe essere integrato nei processi decisionali di ogni organizzazione**. Lo sostiene l'OCSE nella nuova **Raccomandazione sulla sicurezza digitale e la gestione del rischio**. Un ambiente digitale globale, interconnesso, aperto e dinamico genera notevoli opportunità economiche, ancora più promettenti se si pensa alla crescente diffusione dell'Internet delle cose e dei Big Data.

Tuttavia, Paesi e aziende sono esposti a minacce sempre più sofisticate e crescenti che possono mettere in pericolo la sicurezza delle informazioni e compromettere la prosperità economica e sociale.

OCSE a imprese e Governi: considerare la sicurezza informatica un rischio economico

L'OCSE, la cui ultima Raccomandazione sulla sicurezza digitale risale al 2002, indica otto principi-guida per la gestione del rischio riferito alla sicurezza digitale, anche con riguardo alla responsabilità dei diversi soggetti, alla cooperazione tra le parti interessate ed al ruolo dell'innovazione.

In particolare, l'OCSE raccomanda **l'adozione di piani nazionali** per individuare le misure utili a prevenire, individuare, affrontare e sanare le conseguenze di incidenti di sicurezza digitale.

La **Sicurezza delle Informazioni** è assicurata dal binomio inscindibile:
Misure tecnologiche + Procedure adeguate

Condizioni generali per irrogare sanzioni amministrative

Sanzioni da € 10.000.000 a € 20.000.000 o dal 2% al 4% del fatturato mondiale nel caso in cui siano violati:

- Principi relativi al trattamento e al consenso
- Disposizioni relative ai diritti dell'interessato
- Disposizioni in materia di trasferimento dati
- Ordine di cessazione del trattamento

Si lascia agli stati membri il compito di disciplinare le regole e l'effettiva applicazione delle sanzioni amministrative.

Titolare e misure di sicurezza

Tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il responsabile Titolare del trattamento mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati è conforme al regolamento.

- Tali misure sono riesaminate ed aggiornate qualora necessario.
- Tali misure includono politiche adeguate in materia di protezione dei dati.

Sicurezza Informatica nella GDPR

Tra le misure di sicurezza in capo al Titolare e al Responsabile:

Tutela dati personali
by design e *by default*

- Viene introdotto l'obbligo di applicazione di entrambi i principi (*by design* e *by defalut*), non escludendo uno l'applicazione dell'altro.

Privacy fin dalla progettazione:

- Minimizzazione e data retention;
- Sicurezza costante per l'intero ciclo vita dell'informazione;
- Trasparenza verso l'interessato/utente;

Joint Controller

Contitolari

- quando due o più Titolari determinano congiuntamente le finalità e le modalità del trattamento

Gli obblighi che ne discendono:

- Stipula di un accordo interno che, in modo trasparente, determini le reciproche responsabilità in merito all'adempimento degli obblighi del Regolamento (es. esercizio dei diritti, obblighi informativi ecc…);
- Gli interessati devono aver contezza dei tratti generali dell'accordo stipulato.
- Le medesime considerazioni nei contratti per i servizi corporate.

Il rapporto tra il Titolare, i Fornitori/Responsabili ed i sub-Fornitori/ sub-Responsabili

Il Titolare può ricorrere solo a Responsabili che assicurino misure tecniche ed organizzative idonee a soddisfare il rispetto del Regolamento.

L'esecuzione del trattamento su commissione deve essere disciplinato da un contratto che contempli, la durata del trattamento, la sua natura e finalità, le tipologie di dati e le categorie di interessati, i crismi di sicurezza e la relativa ripartizione (PLA), l'obbligo per il responsabile di rispettare i principi del Regolamento, la cancellazione e la restituzione dei dati, il ***data breach***, audit e ***accountability*** a carico del Responsabile ecc…

In base alle decisioni assunte su finalità e modalità, c'è una valutazione effettiva della titolarità a prescindere da quanto formalizzato.

Privacy Impact Assessment e WP 29

Obbligo di PIA quando il trattamento

- Venga effettuato con nuove tecnologie
- Presenti un rischio per i diritti e le libertà fondamentali dell'interessato
- Riguardi la profilazione
- Riguardi categorie particolari di dati (es. biometrici)
- Riguardi la sorveglianza di zone accessibili al pubblico
- Altre ipotesi decise e pubblicate dall'Autorità

Sentito il DPO, il Titolare nella PIA deve tener conto degli impatti del trattamento sui diritti dell'interessato in un'ottica di adempimento agli obblighi del Regolamento anche relativamente all'operato dei fornitori e dei sub-fornitori, tenuto conto dei Pareri dei WP29.

Notifica data breach ad Autorità competente/interessato

Gli obblighi di notifica seguente a data breach vengono estesi a qualsiasi caso in cui vi siano rischi di violazione dei dati personali.

Viene poi esteso l'obbligo di darne comunicazione all'interessato nel caso in cui vi sia rischio elevato per i diritti e le libertà dello stesso.

I tempi di comunicazione sono vaghi (*undue delay*). **Rimangono comunque esclusi:**

Trasferimento dati fuori dai confini europei

- Trasferimento previa decisione adeguatezza;
- Binding Corporate Rules (a condizione che: siano giuridicamente **vincolanti** per tutte le società parti del **Gruppo** di impresa; conferiscano espressamente agli interessati i **diritti** in relazione al trattamento dei loro dati personali; soddisfino i requisiti relativi alle indicazioni sul **contenuto minimo**);
- **Sentenze**;

- Se l'interessato ha prestato il proprio **consenso** informato e specifico al trasferimento;
- Se il trasferimento è funzionale all'adempimento di **obblighi contrattuali** tra Titolare e interessato ovvero per la conclusione di un contratto concluso nell'interesse dell'interessato;
- Per ragioni di **pubblico interesse**, esercizio dei diritti di difesa.

L’analisi per l’adozione del DPO

Dimostrabilità dei parametri assunti

Conservazione delle motivazioni adottate circa l’esito di adozione o meno del DPO

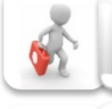
Data Protection Officer

REQUISITI E POSIZIONE

Competenze legali;

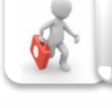
Competenze informatiche;

Conoscenza del settore di mercato dove operano il Titolare o il Responsabile;



Può essere interno o esterno, e può svolgere anche altri compiti;

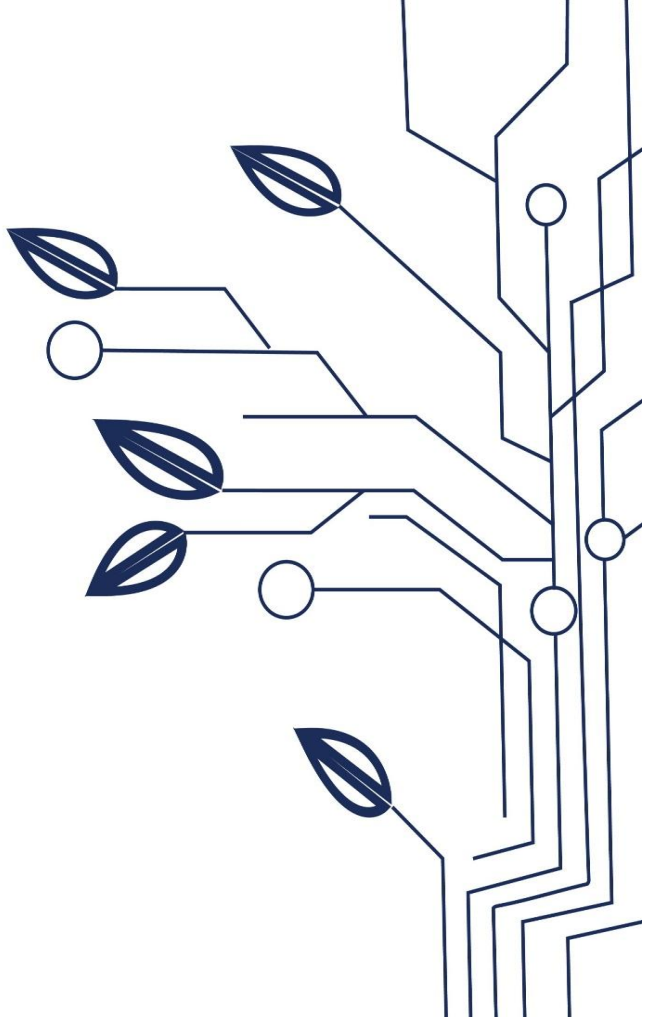
Non deve ricevere istruzioni in merito ai propri compiti e non può essere dimesso o penalizzato;



Riferisce al CdA.

COLIN

CONSULENTE LEGALE INFORMATICO



Privacy e tutela delle informazioni

Diritto informatico

Digitalizzazione

Colin & Partners

Intellectual property

Sorveglianza e controllo

Modello 231 e reati informatici

LaaS - Legal as a Service

DPO

Marketing & Communication

COLIN THINKFACTORY Think Factory

Grazie!

Avv. Valentina Frediani

vfrediani@consulentelegaleinformatico.it

https://it.linkedin.com/in/vfrediani https://twitter.com/fredianivale

Contatti

Sede legale e amministrativa:
Via Cividale, 51 – Montecatini Terme (PT) 51016
Tel. +39 0572 78166
Fax +39 0572 294540
Partita Iva e Codice Fiscale: 01651060475
Le nostre sedi: Montecatini Terme (PT), Milano

www.consulentelegaleinformatico.it

Per richieste progetti e preventivi:
info@consulentelegaleinformatico.it
Per organizzare eventi:
comunicazione@consulentelegaleinformatico.it
Per organizzare corsi di formazione:
thinkfactory@consulentelegaleinformatico.it

Seguici su: