Adempimenti e nuova normativa privacy (GDPR)

Le disposizioni in materia di Protezione dei Dati previste dal Regolamento Comunitario GDPR 2016/679 si applicano a far data dal 25 maggio 2018

Relatore:
Marazzini Raja
Master of Laws (LL.M.)

web
https://www.marazzini.eu/

Relatore e contatti

Marazzini Raja
Master of Laws (LL.M.),

Esperto specializzato su temi di Privacy e di Trattamento dei Dati Personali, curioso delle evoluzioni di A.I. e OSINT (metadati), professionista per la tutela del Know-How e della riservatezza delle informazioni aziendali (asset intangible, N.D.A., etc.), Mobile & Digital, Copyright, Proprietà industriale e intellettuale, Tutela del Design, pratiche per autorizzazioni ad installare Sistemi Biometrici e di Videosorveglianza.
Data Protection Officer (DPO) e Consulente Privacy per aziende, enti ed attività nazionali ed internazionali.

dpo.marazzini.eu
gdpr.marazzini.eu

Aspetti pratici della protezione dei dati

01

Sicurezza, Organizzazione e riservatezza

02

Sottrazione di password e/o informazioni

Aspetti pratici della protezione dei dati

FOCUS DATI SENSIBILI:
SONO TASSATIVI E SONO
QUEI DATI IDONEI A RIVELARE:
1- Origine razziale od etnica;
2- Orientamento religioso
3- Orientamento sessuale
4- L'adesione a partiti politici e/o sindacati
5- Lo stato di salute di una persona

03

Attacchi informatici, truffe on line, phising

04

Utilizzo illecito di dati particolari:

- **dati sensibili**
- **dati di profilazione (introdotti dal GDPR, abitudini di acquisto, gusti personali, etc.)**

Aspetti pratici della protezione dei dati

.....Da dove partiamo?

... 2050...

Art. 2050 - (Responsabilità per l'esercizio di attività pericolose).

Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.”

Il quadro delle fonti

Dalla Direttiva “Madre” D. 95/46/CE (ora abrogata) al Regolamento.
Le attuali fonti in materia di Data Protection sono le seguenti:

01 Regolamento (UE) GDPR 2016/679 del 23 aprile 2016 General Data Protection Regulation

02 D. Lgs. 196/2003 come novellato dal D. Lgs. 101/2018 del 10/08/2018
D. Lgs. 101/2018 in vigore dal 19 settembre 2018: decreto di attuazione su aspetti particolari per i quali il GPDR
ha lasciato piccoli spazi di autonomia ai 28 Paesi Membri

Le figure chiave del GDPR

- Titolare del Trattamento
- Soggetto Autorizzato al trattamento (nomina per i dipendenti)
- Responsabile Esterno del Trattamento (soggetti esterni all'azienda)

In organizzazioni complesse e strutturate è possibile costruire un organigramma ad uso interno affinché la gestione dei dati sia coordinata

- Nomina Responsabili del Trattamento (Referenti per strutture con sedi diverse e/o dati particolari)

- Nomina Sub-Responsabili del Trattamento (Referenti in specifici uffici, dipartimenti, etc.)

DPO (o RPD): Data Protection Officer

- figura introdotta dal GDPR, nominato dal Titolare, risponde al Legale Rappresentante, viene dichiarato all'Autorità Garante Privacy

- **Obbligatorio avere un DPO se:**
  - ente pubblico
  - grande azienda
  - azienda che tratta dati particolari su larga scala

I suoi compiti principali sono:

- definire le migliori strategie di gestione dei dati
- gestire il coordinamento degli adempimenti ai fini della compliance
- rilasciare pareri
- gestire insieme al personale interno i Data Breach

Gli Adempimenti

Necessari per raggiungere una compliance=conformità alle disposizioni del GDPR:

- Informativa e Consenso (informato, libero, specifico, inequivocabile)
- Nomine quali soggetti autorizzati al trattamento
- Nomine soggetti esterni che trattano dati del Titolare del trattamento
- Obbligo per il Titolare ed il Responsabile del Trattamento di adottare misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio (art. 32 par. 1)
- Obbligo per il Titolare di Formare ed informare i propri dipendenti in materia di Protezione dei dati (art. 32 par. 4 Piano formativo interno)
- Tenere un Registro dei Trattamenti (modalità, finalità, protezione)
- Videosorveglianza e Geolocalizzazione solo a determinate condizioni.
- Tenere un Registro delle Violazioni (Data Breach – nel caso di un attacco informatico il titolare entro 72 ore deve comunicare al Garante Privacy l'avvenuta violazione ai propri sistemi/dati)
- Verificare periodicamente l'efficienza delle misure implementate con report trimestrali, semestrali ed annuali per migliorare le strategie.

I comportamenti

I Soggetti Autorizzati al Trattamento Dati devono tenere comportamenti che limitino:

- i rischi di incidente
- la violazione dei dati
- la compromissione della business continuity osservando le disposizioni, i regolamenti ed i mansionari specifici predisposti dal Titolare o dal Responsabile

I comportamenti

- Mantenere riservate le credenziali assegnate;
- Evitare di divulgare informazioni personali e particolari di cui sono venuti a conoscenza nell’esercizio delle funzioni;
- Porre attenzione all’utilizzo della posta elettronica ed evitare di aprire email con contenuti sospetti (consultarsi con colleghi e/o IT)
- Ridurre al minimo l’utilizzo di dispositivi esterni quali chiavette USB o memorie esterne che possono essere sottratte illecitamente;
- Non comunicare via email informazioni e/o trasferire documenti contenenti dati riservati se non a destinatari definiti;
- Non utilizzare dispositivi elettronici senza password di accesso, in caso di furto non vi sarebbe alcuna protezione adeguata;
- Evitare la navigazione su siti web che possano presentare pericoli per il proprio pc/dispositivo

Riferimenti

1- Data Breach - i peggiori della storia (Yahoo 2013 un data breach con 3B di dati compromessi, Collection #1 2019 con 2,7B di dati)

- https://en.wikipedia.org/wiki/List_of_data_breaches

2- Le peggiori password:

- https://nordpass.com/it/most-common-passwords-list/

- https://www.smartworld.it/internet/peggiori-password-2018.html

3- Verifica E-MAIL presenti in data breach noti:

- https://haveibeenpwned.com/

4- Verifica PASSWORD oggetto di data breach:

- https://haveibeenpwned.com/Passwords

5- Spot su diffusione dei dati personali nei social network e su web:

- https://www.youtube.com/watch?v=qYnmfBiomlo

Questionario di valutazione (rispondere Vero/Falso)

1. Il Regolamento (UE) GDPR è direttamente applicabile nei 28 paesi (27+1 post brexit UK).
2. Il Titolare del Trattamento non è tenuto ad adottare misure di sicurezza adeguate.
3. Il soggetto autorizzato al trattamento può comunicare le sue password ai colleghi.
4. Il dipendente che utilizza un computer windows connesso ad internet può disattivare l’antivirus per essere più veloce.

5. Il Titolare del Trattamento può utilizzare un impianto di videosorveglianza per controllare il lavoro dei propri dipendenti.

6. Informazioni di business e know-How aziendale possono essere divulgate alle aziende competitor.

7. Il dipendente che ruba dati sensibili per rivenderli non è perseguibile.

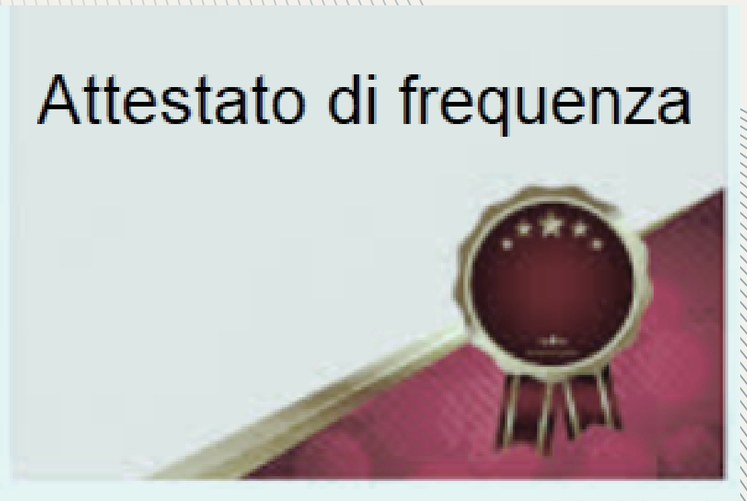
8. Le sanzioni del GDPR possono arrivare al 4% del fatturato annuo di gruppo

9. Le violazioni dei dati (i c.d. Data Breach) non riguardano le grandi società internazionali.

10. Il registro delle violazioni non deve essere aggiornato nel tempo.

Questionario di valutazione (si supera con 8 su 10)

ATTESTATO CORSO BASE DI 4 ORE
GDPR 2016/679



Dott. Raja Marazzini
dpo.marazzini.eu
gdpr.marazzini.eu

Grazie!

In caso di domande o necessità di chiarimenti potete scrivere al relatore all’indirizzo:

raja.marazzini@icloud.com