Protezione dati e privacy

Baroum Mrad

La Protezione dati e Privacy

«…privacy come valore attorno al quale ricostruire un nuovo patto sociale: anello di congiunzione tra pubblico e privato, precondizione di ogni altro diritto civile, sociale, persino politico nella "società dell'informazione".» -
Giovanni Buttarelli, garante Europeo della protezione dei dati (2014-2019)

Protezione dati

Misure di sicurezza per la protezione dei dati personali (Data Protection)

Privacy

Misure di sicurezza per garantire la protezione della sfera privata. (Diritto umano)

La Protezione dati e Privacy

Protezione Dati

TECHNICAL MEASURES

INFORMATION SECURITY

- Confidenzialità, integrità, disponibilità
- Governance dei dati (concetto di protezione dati)
- Sicurezza dei dati
  - Incident and Data Breach Response Policy
  - Notifica di violazioni della sicurezza dei dati
  - Anonimizzazione e pseudinimizzazione
- Registro delle attività di trattamenti dei dati personali
  - Subappalto di trattamento dei dati (DPA)
- Vendor / Supplier Management
  - P.es. Medical Devices
- Enterprise Mobile Management (EMM)

Privacy

LA PERSONA

PRIVACY MANAGEMENT

- Implementazione di un programma Privacy con un registro centrale per la governance e compliance dei dati.
- Responsabilità.
- Gestione dei consensi (consenso generale e consenso per la ricerca)
- Privacy by Design e Privacy by Default
  - Valutazione d'impatto (DPIA)
- Gestione dei diritti della persona
  - Diritto di accesso alla cartella clinica
- Gestione rischi

La Protezione dati e Privacy

FISICA

INFORMAZIONI

DECISIONALE

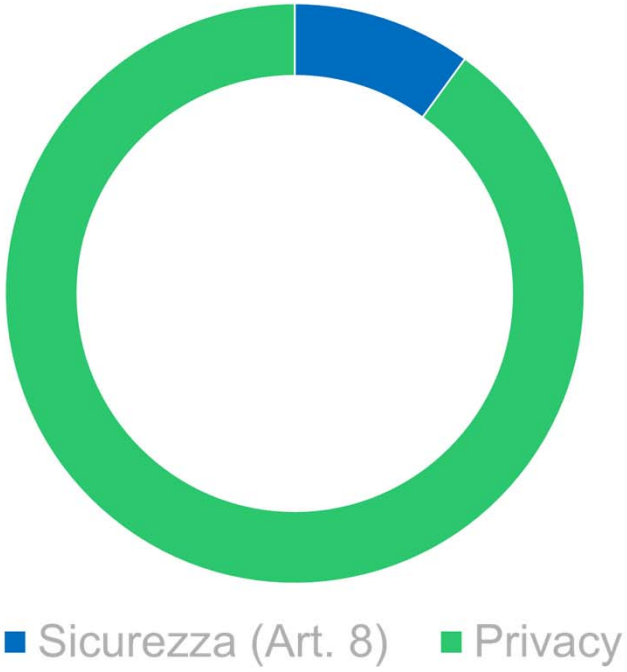
La Protezione dati e Privacy

Privacy vs Security

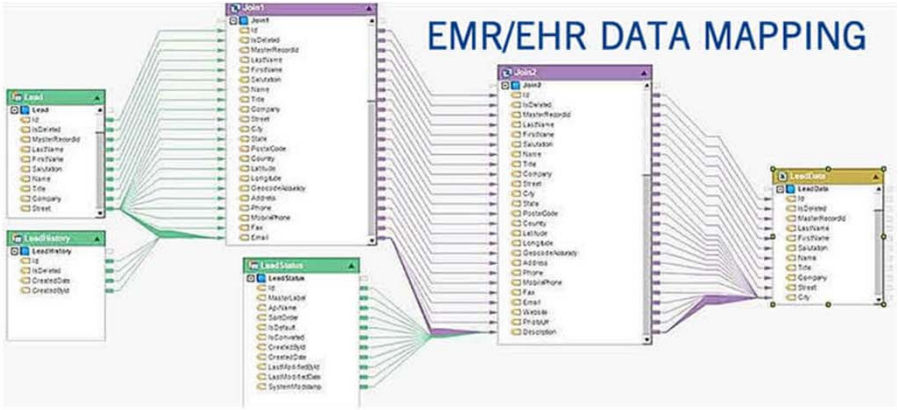
Perché è importante distinguere tra Privacy e Sicurezza?

Art. 8 nLPD (adottato il 25.9.2020)
Sicurezza dei dati

1. Il responsabile e la persona che tratta l'ordine garantiscono una sicurezza dei dati commisurata al rischio mediante adeguate misure tecniche e organizzative.
2. Le misure devono consentire di evitare violazioni della sicurezza dei dati.
3. Il Consiglio federale stabilisce le prescrizioni minime per la sicurezza dei dati.



La Protezione dati e Privacy



Art. 12 della LPD

Tenuta **del registro della attività di trattamento** contenente le principali informazioni relative alle operazioni di trattamento svolte dal titolare, e dove presente dal responsabile, del trattamento.

Cpv. 5 è prevista un'eccezione per le seguenti aziende:

- Meno di 250 collaboratori;
- Trattamenti di dati personali effettuati comportano un rischio esiguo di violazione della personalità delle persone interessate.

Non specifica nel registro la durata della conservazione dei dati, ma non esonera l'azienda dallo stabilire e applicare i termini di conservazione, distruzione, anonimizzazione (art. 6 cpv 4 LPD).

La Protezione dati e Privacy

EU GDPR

Scope:
EU regulation focusing on general data protection related to the processing of personal data in the private and public sectors

Status: ratified and in force
In effect since: 25 May 2018

ePrivacy

Scope:
EU regulation with focus on data protection on the Internet and in electronic communications

Status: Draft in ratification by the European Parliament and the Council of Europe
In effect from: 2020 (expected)

Federal Act on Data Protection (FADP)

Scope:
Swiss federal law with focus on general data protection in connection with the processing of personal data in the private and public sectors

Status: Draft in ratification at the Swiss Federal Assembly
In effect from: 2019 (expected)

La Protezione dati e Privacy

Tre dimensioni della sicurezza informatica

- **Dimensione 1 - Interpretare la legge**
  - Scrivere politiche e procedure per conformarsi
    - Conformità interna (internal compliance) e protezione da atti esterni

- **Dimensione 2 - Conformità interna (internal compliance)**
  - Verificare che la politica e le procedure di conformità interna siano correttamente implementate

- **Dimensione 3 - Conformità esterna (external compliance)**
  - Verificare che la politica e le procedure di protezione dalle intrusioni esterne e le procedure sono implementate correttamente

La Protezione dati e Privacy

1. Stabilire un quadro normativo e un quadro di governance (Governance Framework) - awareness consiglio di amministrazione e top management, registro dei rischi, registro dei dati, quadro di responsabilità (Accountability Framework), revisione continua (Audit)
2. Nominare e formare un responsabile della protezione dei dati (DPO)
3. Condurre un audit del flusso di dati e creare un inventario dei dati (registro) - identificare i processori e tutti i dati detenuti illegalmente (data mapping)
4. Analisi della gap di conformità (gap analysis)
    a) Garantire che i documenti, Privacy Policy e Notice, e i processi SAR siano solidi e leciti (conformi)
    b) Registro dei trattamenti dei dati
5. Sviluppare politiche, procedure e processi operativi in linea con le migliori pratiche di sicurezza informatica (InfoSec)
6. Aggiornare il materiale di comunicazione e formare il personale sui requisiti del regolamento
    a) Quadro di riferimento per la conformità alla normativa sulla privacy
    b) Cyber Essentials/Deci passi verso la Cyber Security/ISO 27001 (ISO27701)
7. Data Breach Response Process (testare e praticare annualmente!)
8. Monitorare, controllare e migliorare continuamente

La Protezione dati e Privacy

I benefici diretti di un programma di data *governance* solido

- Allineare strategicamente gli sforzi di sicurezza con le strategie aziendali per sostenere gli obiettivi dell'organizzazione;
- Sostenere la gestione del rischio applicando i controlli necessari per mitigare i rischi;
- Ridurre l'impatto delle violazioni della sicurezza sulle risorse informative; e
- Migliorare la gestione delle risorse gestendo in modo efficiente la sicurezza conoscenza e infrastrutture.

Una *governance* efficace, con un focus sulla mitigazione del rischio

- Maggiore controllo sulla riservatezza, integrità e disponibilità dei dati e ciò comporta un minor potenziale di responsabilità civile o legale;
- un'allocazione più efficiente in termini di costi delle risorse di sicurezza;
- Miglioramenti nella gestione del rischio, nei processi aziendali e nella risposta all'incidente in caso di violazione;
- la capacità di prendere decisioni critiche sulla base di informazioni chiare e valide; e
- Maggiore tutela delle informazioni sensibili durante le attività importanti attività, come acquisizioni e fusioni, risposte normative e recupero del processo di business.

La Protezione dati e Privacy

Human Error: 33.5%

"The larger problem is that people are not being cautioned about cybersecurity. ... If you're not training people well, no matter what technology you have, you're only creating future problems. ...Make the investment." – Santiago Lopez, Ethical Hacker

La misura più importante per prevenire e proteggere i dati personali è sicuramente la consapevolezza e la formazione continua. Awareness e Training riducono enormemente i rischi di protezione dati e Cyber Attacks.