Appunti TPS: Gestione Dati tra GDPR e AI

---

1. Introduzione al GDPR

Definizione e contesto normativo

Il **GDPR** (General Data Protection Regulation) è il Regolamento UE 2016/679 entrato in vigore il 25 maggio 2016 e applicato dal 25 maggio 2018. Rappresenta la principale normativa europea per la protezione dei dati personali.

Principi fondamentali del GDPR

1.1 Accountability (Responsabilizzazione)

- Il titolare del trattamento è **responsabile** della scelta e attuazione di misure tecniche e organizzative
- Deve **dimostrare** la conformità al regolamento
- Principio: "Fai tu, ma se si creano problemi ne rispondi"

1.2 Privacy by Design

- Protezione incorporata nella **progettazione** del sistema
- Caratteristiche di protezione configurate al **massimo livello** fin dall'inizio
- Prevenzione dei problemi invece che correzione a posteriori

1.3 Privacy by Default

- Trattamento **solo dei dati necessari** per le finalità previste
- Per il **periodo strettamente necessario**
- Configurazioni predefinite orientate alla privacy

1.4 Data Breach Prevention & Detection

- Misure di sicurezza adeguate per la **prevenzione**
- Capacità di **riconoscere** gli incidenti di sicurezza
- **Notifica** al Garante Privacy entro 72 ore

---

2. Architettura tecnica per la conformità GDPR

2.1 Implementazione SSL/TLS

```
Requisiti minimi:
- Certificato SSL DV (Domain Validated)
- Redirect forzato da HTTP a HTTPS
- Crittografia dei canali di comunicazione
```

2.2 Architettura a 3 livelli

- **Presentation Layer**: Interfaccia utente
- **Business Logic Layer**: Elaborazione dati
- **Data Layer**: Storage e persistenza

Vantaggi: separazione delle responsabilità, specializzazione dei server, maggiore sicurezza.

2.3 Sistemi di backup e tracciamento

- Backup automatizzati dei dati
- Email tracciate con registro
- Log delle operazioni sui dati personali

---

3. Gestione dei ruoli e responsabilità

3.1 Figure chiave nel trattamento dati

Titolare del trattamento

- **Responsabilità legale** del trattamento
- Definisce finalità e modalità
- Risponde delle violazioni

Responsabile del trattamento

- Tratta i dati **per conto** del titolare
- Segue le istruzioni del titolare
- Applica misure di sicurezza adeguate

Incaricati del trattamento

- Operatori che **materialmente** trattano i dati
- Necessitano di **lettera di incarico** specifica
- Autorizzati solo per operazioni definite

DPO (Data Protection Officer)

- **Non obbligatorio** per PMI (<250 dipendenti)
- Consigliato per maggiore compliance
- Funzioni di controllo e consulenza

---

4. Gestione tecnica dei dati personali

4.1 Classificazione dei dati

```
Dati comuni: nome, cognome, indirizzo, telefono
Dati particolari (art. 9): salute, orientamento politico/religioso
Dati giudiziari: condanne penali, procedimenti
```

4.2 Pseudonimizzazione

Tecnica che **separa** i dati identificativi dalle altre informazioni, riducendo i rischi in caso di violazione.

Esempio pratico:

```
Invece di: "Mario Rossi, via Roma 1, diabetico"
Usare: "ID001 → Mario Rossi, via Roma 1" + "ID001 → diabetico"
```

4.3 Misure di sicurezza tecniche

Controllo degli accessi

- Autenticazione forte (password + 2FA)
- Profilazione utenti per livelli di accesso
- Log degli accessi ai sistemi

Protezione dei sistemi

- Firewall perimetrali
- Antivirus aggiornati
- Patch di sicurezza regolari
- Crittografia dei dati sensibili

---

5. Informativa e consenso

5.1 Contenuti dell'informativa (art. 13 GDPR)

- Identità del titolare del trattamento
- **Finalità** e base giuridica del trattamento
- Categorie di dati trattati
- Destinatari dei dati
- Tempi di conservazione
- **Diritti** dell'interessato

5.2 Modalità di comunicazione

- Linguaggio **chiaro e semplice**
- Facilmente accessibile
- Gratuita per l'interessato
- Aggiornata costantemente

---

6. Diritti dell'interessato

6.1 Diritti tradizionali

- **Accesso**: ottenere copia dei propri dati

- **Rettifica**: correggere dati inesatti
- **Cancellazione**: "diritto all'oblio"

6.2 Nuovi diritti GDPR

- **Portabilità**: trasferire dati tra servizi
- **Limitazione**: bloccare certi trattamenti
- **Opposizione**: rifiutare il trattamento

6.3 Tempi di risposta

- **1 mese** per rispondere alle richieste
- Estendibile a 3 mesi in casi complessi
- Comunicazione **gratuita** salvo richieste eccessive

---

7. GDPR e Intelligenza Artificiale

7.1 Sfide specifiche dell'AI

- **Profilazione automatizzata**: decisioni basate su algoritmi
- **Black box**: difficoltà di spiegare le decisioni AI
- **Bias algoritmici**: discriminazioni non intenzionali
- **Scalabilità**: trattamento di grandi volumi di dati

7.2 Requisiti per sistemi AI

Trasparenza algoritmica

- Informare sulle **logiche** di funzionamento
- Spiegare i **fattori** considerati nelle decisioni
- Garantire **comprensibilità** all'interessato

Diritto di non essere sottoposti a decisioni automatizzate

- L'interessato può **opporsi** a decisioni solo algoritmiche
- Diritto di **intervento umano** nel processo decisionale
- **Contestazione** delle decisioni automatiche

7.3 Privacy by Design nell'AI

Minimizzazione dei dati

```
# Esempio concettuale
# Invece di raccogliere tutti i dati disponibili:
dati_utente = ["nome", "età", "reddito", "hobbies", "famiglia", ...]

# Raccogliere solo il necessario per lo scopo:
dati_necessari = ["età", "reddito"]  # Per un sistema di credit scoring
```

Anonimizzazione e aggregazione

- Tecniche di **differential privacy**
- **Aggregazione** statistica dei dati
- **Synthetic data** per training AI

---

8. Gestione delle violazioni (Data Breach)

8.1 Procedura di gestione

Fase 1: Rilevamento (entro 72h)

- Identificare la **natura** della violazione
- Stimare **numero** di interessati coinvolti
- Valutare **probabili conseguenze**

Fase 2: Notifica

- **Garante Privacy**: entro 72h se rischio elevato
- **Interessati**: senza ritardo se rischio elevato
- **Documentazione** interna sempre obbligatoria

Fase 3: Contenimento e correzione

- **Isolare** i sistemi compromessi
- **Correggere** le vulnerabilità
- **Implementare** misure preventive

8.2 Registro delle violazioni

Documenti da mantenere:

- Data e ora della violazione
- Tipologia di dati coinvolti
- Numero di interessati
- Misure adottate
- Comunicazioni effettuate

---

9. Valutazione d'impatto sulla protezione dei dati (DPIA)

9.1 Quando è obbligatoria

- Trattamenti con **alto rischio** per diritti e libertà
- **Profilazione sistematica** su larga scala
- Trattamento di **dati particolari** su larga scala
- **Sorveglianza sistematica** di aree pubbliche

9.2 Metodologia DPIA

Step 1: Descrizione del trattamento

- Finalità e modalità
- Tipologie di dati
- Soggetti coinvolti
- Tecnologie utilizzate

Step 2: Valutazione necessità e proporzionalità

- Conformità ai principi GDPR
- Bilanciamento interessi
- Alternative meno invasive

Step 3: Identificazione e valutazione rischi

```
Rischio = Probabilità × Impatto
Livelli: Basso, Medio, Alto, Molto Alto
```

Step 4: Misure di mitigazione

- Misure tecniche
- Misure organizzative
- Garanzie aggiuntive

---

10. Sanzioni e compliance

10.1 Sistema sanzionatorio

- **Livello 1**: fino a 10M€ o 2% fatturato annuo
- **Livello 2**: fino a 20M€ o 4% fatturato annuo
- Si applica l'**importo maggiore**

10.2 Fattori aggravanti/attenuanti

Aggravanti:

- Violazioni intenzionali
- Mancata cooperazione con autorità
- Violazioni precedenti

Attenuanti:

- Collaborazione proattiva
- Misure tecniche e organizzative adeguate
- Notifica tempestiva delle violazioni

---

11. Casi pratici e esempi

11.1 Sviluppo di un'app mobile

Scenario: App per food delivery con geolocalizzazione

Considerazioni GDPR:

- Informativa chiara su uso GPS
- Consenso per notifiche push
- Minimizzazione dati: solo posizione necessaria per consegna
- Cancellazione automatica dati di geolocalizzazione dopo consegna

11.2 Sistema di videosorveglianza smart

Scenario: Telecamere con riconoscimento facciale

Considerazioni GDPR:

- DPIA obbligatoria (alto rischio)
- Informativa visibile e comprensibile
- Bilanciamento tra sicurezza e privacy
- Limitazione conservazione registrazioni (24-72h massimo)
- Diritti dell'interessato: accesso, cancellazione

11.3 Chatbot con AI

Scenario: Assistente virtuale per customer service

Considerazioni GDPR:

- Trasparenza: informare che è un bot
- Limitare raccolta dati alle finalità del servizio
- Diritto di intervento umano
- Gestione richieste di cancellazione conversazioni

---

12. Strumenti e tecnologie per la compliance

12.1 Privacy Management Software

- **Consent Management Platform** (CMP)
- **Data Loss Prevention** (DLP)
- **Privacy Impact Assessment** tools

12.2 Tecnologie privacy-preserving

- **Homomorphic encryption**: calcoli su dati cifrati
- **Secure multi-party computation**: elaborazioni distribuite sicure
- **Zero-knowledge proofs**: dimostrazioni senza rivelare informazioni

12.3 Blockchain e privacy

- **Immutabilità vs diritto all'oblio**: contraddizione tecnica
- Soluzioni: **off-chain storage**, **hash pointers**
- **Self-sovereign identity**: controllo diretto dei propri dati

---

13. Conclusioni e tendenze future

13.1 Evoluzione normativa

- **AI Act** europeo in via di definizione
- **Digital Services Act** e **Digital Markets Act**
- Armonizzazione internazionale delle normative privacy

13.2 Sfide tecnologiche emergenti

- **IoT** e privacy: miliardi di dispositivi connessi
- **Edge computing**: elaborazione distribuita e controllo dati
- **Quantum computing**: nuove sfide crittografiche

13.3 Il ruolo del tecnico informatico

- **Privacy by design** come competenza core
- **Ethical AI development**: responsabilità professionale
- **Continuous learning**: normative in costante evoluzione

Glossario tecnico

Accountability: Principio di responsabilizzazione del titolare del trattamento

Breach: Violazione di sicurezza che comporta perdita, alterazione o accesso non autorizzato ai dati

Consent: Manifestazione di volontà libera, specifica, informata e inequivocabile

Controller: Titolare del trattamento che determina finalità e modalità

Data Subject: Interessato, persona fisica cui si riferiscono i dati personali

DPIA: Data Protection Impact Assessment, valutazione d'impatto sulla protezione dei dati

DPO: Data Protection Officer, responsabile della protezione dei dati

Lawful basis: Base giuridica del trattamento (consenso, contratto, interesse legittimo, etc.)

Personal Data: Qualsiasi informazione riguardante una persona fisica identificata o identificabile

Processor: Responsabile del trattamento che tratta i dati per conto del titolare

Profiling: Trattamento automatizzato per valutare aspetti personali di una persona fisica

Pseudonymisation: Trattamento che impedisce l'attribuzione a un interessato senza informazioni aggiuntive

Supervisory Authority: Autorità di controllo (in Italia: Garante Privacy)