Privacy-by-default
e
Privacy-by-design

Prof. Antonio Lioy

< lioy @ polito.it >

Politecnico di Torino

Dip. Automatica e Informatica

EU-GDPR art. 25 par. 1

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento,

come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento,

sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace

i principi di protezione dei dati, quali la minimizzazione, e

a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

EU-GDPR art. 25 par. 1 – conseguenze

- **stato dell'arte …**
  - aggiornamento continuo
- **rischi …**
  - analisi dei rischi formalizzata (ed aggiornata)
- **misure tecniche ed organizzative …**
  - soluzioni tecniche reali
  - procedure (e comportamenti individuali!)
- **protezione dei dati …**
  - non solo minimizzazione
- **integrare nel trattamento ...**
  - protezione integrata (non la ciliegina sulla torta!)

EU-GDPR art. 25 par. 2

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita (default),

solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per:

- **la quantità dei dati personali raccolti,**
- **la portata del trattamento,**
- **il periodo di conservazione e**
- **l'accessibilità.**

In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Privacy by design

- **ogni servizio o processo di business che usa dati personali deve considerare bene la loro protezione nella fase di progetto (ed implementazione)**
- **bisogna essere in grado di dimostrare che:**
  - ci sono adeguate misure di sicurezza
  - viene continuamente verificato il rispetto del principio di privacy
- **in pratica il dipartimento IT deve mirare a proteggere i dati personali durante tutto il ciclo di vita dei dati, dei sistemi e dei processi**
- **responsabilizzazione di chi effettua il trattamento dei dati**

Privacy by default

- **le impostazioni più restrittive devono essere applicate automaticamente**
  - il cliente non deve fare niente per proteggere la propria privacy
  - eventualmente il cliente può fare qualcosa se desidera che i propri dati vengano divulgati
- **i dati devono essere conservati solo per il tempo strettamente necessario a fornire il servizio**
  - il cliente non deve fare niente per veder cancellati i propri dati una volta terminato il rapporto col fornitore
- **OPT-IN … non OPT-OUT !**

Privacy-by-design in pratica (I)

- **normalmente privacy (e sicurezza) non considerate nella fase inziale dei progetti IT**
- **Ann Cavoukian (ex Information and Privacy Commissioner of Ontario) ha definito sette principi**
- **1. Proactive not reactive**
  - prevedere implica analisi dei rischi
- **2. Privacy as the default setting**
  - privacy-by-default
- **3. Privacy embedded into design**
  - progetto delle architetture IT, dei processi di business e delle operazioni
  - tecnologie usate nel progetto

Privacy-by-design in pratica (II)

- **4. Full functionality**
  - no trade-off protezione-funzionalità
- **5. Full lifecycle protection**
  - no "buchi" nella protezione o nella accountability
  - acquisizione, memorizzazione e trattamento, sino alla distruzione dei dati
- **6. Visibility and transparency**
  - principio "trust-but-verify" (mi-fido-ma-controllo)
- **7. Respect for user privacy – above all**

EU-GDPR art. 32 par. 1

- **misure tecniche suggerite:**

a) la pseudonimizzazione e la cifratura dei dati personali

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

= cybersecurity + business continuity + disaster recovery

GRAZIE PER L'ATTENZIONE!

DOMANDE?