GDPR IN SANITÀ: LINEE GUIDA AISIS

Misure tecniche

13 Ottobre – Torino

Claudio Telmon

Consulente

Membro del Comitato Tecnico Scientifico e del Comitato Direttivo di Clusit

ctelmon@clusit.it

SICURAMENTE
WWW.CLUSIT.IT

Associazione “no profit” con sede presso
l’Università degli Studi di Milano
Dipartimento di Informatica

2000-2017: 17 anni dedicati alla sicurezza

Principio di accountability e Articolo 32

- Il principio di accountability si applica anche alle misure tecniche
  - Niente elenchi di misure minime
- Sicurezza del trattamento(art. 32):

Tenendo conto dello stato dell'arte e dei **costi di attuazione**, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche **del rischio di varia probabilità e gravità** per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento **mettono in atto misure tecniche e organizzative adeguate** per garantire un livello di sicurezza adeguato al rischio, che comprendono, **tra le altre, se del caso:**

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.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto **in special modo** dei rischi presentati dal trattamento che derivano in particolare *dalla distruzione, dalla perdita, dalla **modifica**, dalla divulgazione non autorizzata o dall'accesso*, in modo **accidentale** o illegale, a dati personali trasmessi, conservati o comunque trattati

Data protection by design (art. 25)

- **Comma 1**) (**concetto di protezione dei dati by design**)……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.

- Comma 2) (**concetto di privacy by default**)…Il Titolare del trattamento mette in atto **misure tecniche ed organizzative adeguate** per garantire che siano trattatati , **per impostazione predefinita, solo i dati personali per ogni specifica attività di trattamento**

- Le repliche non necessarie, l'utilizzo di dati personali in ambiente di test, i flussi con più dati personali (es. di più soggetti o con più informazioni) non sono conformi, i profili di accesso sono definiti e minimi
- Di default, i canali sono protetti (cifrati?), gli accessi non sono consentiti

L’adeguamento non è un’attività one-shot

- Alcuni adeguamenti comportano un cambio di impostazione o di prospettiva
  - Privacy by design & by default
  - Logiche di DPIA nella valutazione dei nuovi progetti
- Altri sono onerosi e saranno oggetto di adeguamento nel tempo:
  - Es. pseudonimizzazione
- Serve però anche valutare delle attività per far **evolvere** il sistema informativo per rendere meno oneroso supportare l’adeguamento

Centralizzazione dei servizi

- L'adeguamento è favorito da una evoluzione verso una gestione centralizzata
  - Delle identità e dei profili (IAM)
  - Dei log di sicurezza
  - Dei consensi
  - Delle anagrafiche degli interessati

    Per supportare/facilitare le modifiche, cancellazioni, aggiornamenti, la pseudonimizzazione ecc., la portabilità, la gestione dei tempi di retention

Centralizzazione dei servizi

- L'adeguamento è favorito da una evoluzione verso una gestione centralizzata
  - Delle identità e dei profili (IAM)
  - Dei log di sicurezza
  - Dei consensi
  - Delle anagrafiche degli interessati

    Per supportare/facilitare le modifiche, cancellazioni, aggiornamenti, la pseudonimizzazione ecc., la portabilità, la gestione dei tempi di retention

Supporto alla gestione dei diritti degli interessati

- diritto all'oblio (art. 17) (conseguenza: ogni raccolta di dati è associata più puntualmente a trattamenti e a tempi di retention)
- Richiamo esplicito sul trasferimento dei dati all'estero
- portabilità dei dati (art. 20):
  - L'interessato ha il diritto di ricevere in un **formato strutturato**, di uso comune e **leggibile da dispositivo automatico** i dati personali che lo riguardano **forniti** a un titolare del trattamento e ha il diritto di **trasmettere tali dati a un altro titolare** del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora…

Impatto sui processi di gestione

- Sviluppo e acquisizione: logiche di protection by design e privacy by default devono entrare nei processi fin dall'inizio, **documentando** la raccolta di requisiti, la valutazione dei rischi e l'applicazione dei principi del GDPR

- Processi di change & configuration management: assicurare la configurazione sicura, **documentando** le attività (es. attraverso ticket)

- Identity Management: ricertificazione periodica dei profili

Incident management

- La gestione dei data breach inizia con la capacità di **rilevare** incidenti che possano danneggiare l'integrità, riservatezza e disponibilità dei dati personali

- Un processo di gestione degli incidenti deve essere efficace nel **rilevare e contenere** l'evento e nel risolverlo tempestivamente

- Tutto questo, oltre alle diverse tematiche organizzative (es. procedura di escalation) richiede l'implementazione di funzionalità di **monitoraggio** del sistema informativo e segnalazione di eventi (potenziali data breach)
  - Non solo intrusioni esterne e malware


15
MPH
Grazie!
Claudio Telmon
ctelmon@clusit.it