UNIVERSITÀ DEGLI STUDI
DI MILANO

Alcune riflessioni su Garante, sanzioni e GDPR

Prof. Giovanni Ziccardi

Information Society Law Center

ASSINTEL, 27 febbraio 2019

1. Prevedibilità delle sanzioni? (1/11)

- Le relazioni annuali del Garante
- I casi più importanti degli ultimi vent'anni
- Le attività dei Garanti in altri Paesi europei

Relazione annuale Garante (2/11)

Abbiamo il dettaglio degli interventi, delle sanzioni, delle tipologie di Titolare «attenzionato»

Quattro grandi ambiti:

- Informativa
- Consenso / trattamento illecito / misure minime
- Data breach
- False comunicazioni al Garante / ostacolo alle sue attività

Informativa: TRASPARENZA (3/11)

Omessa

Non viene data. Perché?

Inidonea

- Non conforme alla legge
- Oscura
- Non specifica per quel trattamento

Consenso / trattamento illecito (4/11)

- Consenso in sé (raccolta chiara, soprattutto online)
- Principi fondamentali (necessità, pertinenza, legalità, non eccedenza)
- Vecchie «misure minime»

Data breach (5/11)

Fenomeno attualissimo e in espansione

- Segnalazione
- Misure precedenti
- Misure immediatamente successive
- Rapporto con gli utenti e trasparenza

Rapporto col Garante (6/11)

- Livello di cooperazione
- Documenti pronti e reali
- Consultazioni preventive
- Registri degli incidenti
- Accountability pronta da mostrare e in ordine

2. Ultimi vent'anni? (7/11)

- Esposizione di dati sensibili su siti web
- Videosorveglianza
- Controllo dei lavoratori
- Data breach
- Marketing selvaggio di tutte le compagnie telefoniche

3. Il futuro? (8/11)

- Informativa e trasparenza su web, app e smartphones
- I minori
- Studi e documenti interni che testimoniano un processo di adeguamento reale e verificabile (registro, valutazione d'impatto, istruzioni ai soggetti autorizzati, contratti con responsabili esterni, policy per gestione dei data breach)

4. Gli altri Paesi (9/11)

- Austria: videosorveglianza. Approccio: **soft** (multe basse, 4.000, cerca di condurre le realtà a compliance)
- Germania: data breach chat online, approccio **soft** (330.000 credenziali in chiaro, 20.000 euro). Piccole aziende impreparate.
- Portogallo: ospedali, approccio **hard** (400.000), politiche di accesso al dato sbagliate, tutti vedevano tutto.

4. Gli altri Paesi (10/11)

- Francia: approccio **hard** con Google, 50 milioni, non trasparenza durante la configurazione dei nuovi smartphones e consenso forzato e troppo complesso / mancanza di trasparenza.

5. Conclusioni (11/11)

- Guardare il **passato**: abbiamo uno storico di oltre vent'anni e l'approccio investigativo non cambierà
- Guardare il **presente**: data breach, app, siti web, controllo, sorveglianza.
- Guardare il **futuro**: i nuovi adempimenti correlati al nuovo approccio. Registro, valutazioni impatto, nuovo approccio alle misure di sicurezza, soluzione di videosorveglianza, lavoratori e amministratori di sistema, responsabili esterni
- Centralità del DPO, modularità estrema della sanzione, istruttoria necessaria: un **buon carattere**!

UNIVERSITÀ DEGLI STUDI
DI MILANO

UNIVERSITÀ
DEGLI STUDI
DI MILANO