Convegno Annuale AISIS

Privacy e Sicurezza
A supporto dell'innovazione digitale in Sanità

Analisi del rischio e degli impatti e profilo sanzionatorio del GDPR

Alessandra Delli Ponti
avvocato

Torino, 12 e 13 ottobre 2017
Hotel NH Torino Centro

DIR 95/46/CEE

…….l'obbligo di rispettare le regole fissate per la liceità dei trattamenti (art. 6) e solo come ulteriore dovere specifico quello di assicurare le misure di sicurezza adeguate

REGOLAMENTO UE

..nel Regolamento il Controller ha invece un ruolo proattivo, finalizzato non solo al rispetto delle regole ma anche alla necessità di dimostrare che ha adottato tutti gli accorgimenti tecnici e organizzativi necessari a garantire la "compliance" dei trattamenti

ACCOUNTABILITY

ART. 5 comma 2

Il titolare del trattamento è competente

per il rispetto del paragrafo 1 e

in grado di comprovarlo («responsabilizzazione")

Sanzioni art. 83

REGIMI SANZIONATORI

Risarcimento del danno art. 82

Chiunque subisca un danno materiale o immateriale

cagionato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno **dal titolare del trattamento o dal responsabile del trattamento.**

Ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento non conforme al presente regolamento **salvo che dimostri che l'evento dannoso non gli è in alcun modo imputabile.**

Un responsabile del trattamento risponde per il danno cagionato dal trattamento solo **se non ha adempiuto gli obblighi del presente regolamento** specificatamente diretti ai responsabili del trattamento o ha agito **in modo esterno o contrario alle legittime istruzioni** del titolare del trattamento.

Alcune osservazioni

⇒ **Il concetto di danno (considerando 146)**

⇒ **Trattamento dati come attività pericolosa ex art. 2050 c.c.**

⇒ **L'azione di regresso**

⇒ **Il ruolo dei contratti**

⇒ **L'importanza dell'analisi del rischio**

⇒ **L'importanza del "sistema" del tracciamento delle operazioni**

Sanzioni Amministrative pecuniarie

fino a € 10.000.000, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per violazione di :

- **(25) Privacy by design e privacy by default**
- **(26) Contitolari del trattamento**
- **(28) Responsabile del trattamento**
- **(30) Registri delle attività di trattamento**
- **(32) Sicurezza del trattamento**
- **(33) e (34) Data Breach**
- **(35) Valutazione d'impatto sulla protezione dei dati**
- **(36) Consultazione preventiva**
- **(37, 38, 39) Designazione (e posizione e compiti...) del DPO**

Sanzioni Amministrative pecuniarie

fino a € 20.000.000, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per violazione di :

- **principi di base del trattamento**, articoli 5, 6, 7 e 9 (Principi applicabili al trattamento di dati personali; Liceità del trattamento; Condizioni per il consenso; Trattamento di categorie particolari di dati personali)
- **diritti degli interessati** (artt. da 12 a 22)
- **trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale** a norma degli articoli da 44 a 49;

SANZIONE AMMNINISTRATIVA PECUNIARIA (art.83)

le sanzioni amministrative pecuniarie inflitte saranno **in ogni singolo caso effettive, proporzionate e dissuasive**

Elementi per la quantificazione della sanzione:

- **la natura, la gravità e la durata della violazione**
- **il carattere doloso o colposo della violazione;**
- **le misure adottate dal titolare del trattamento;**
- **il grado di responsabilità del titolare del trattamento**
- **eventuali precedenti**
- **il grado di cooperazione con l'autorità di vigilanza**
- **le categorie di dati personali interessate dalla violazione;**
- **l'adesione ai codici di condotta**
- **eventuali altri fattori aggravanti o attenuanti**

COME DIFENDERSI?

PREDISPONENDO LE PROVE


Protezione dei dati
Accountability
Modello organizzativo per la gestione dei dati

DISEGNARE UN MODELLO DI GESTIONE DEI DATI

1. Rivedere l'organigramma e i contratti
2. Mappatura dei dati
3. Mappatura dei trattamenti
4. Gestire il rischio
5. Redigere procedure interne
6. Documentare la conformità

Grazie dell'attenzione e buon lavoro