LA SICUREZZA DEI DATI NEL GDPR

03 Maggio 2018

Claudio Telmon

Consulente

Membro del Comitato Tecnico Scientifico e del Comitato Direttivo di Clusit

ctelmon@clusit.it

Immagini: fonte pixabay.com CC0

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

Art. 32: sicurezza del trattamento

1. 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.
…

Sicurezza: principio di accountability e gestione del rischio

- Il regolamento segue logiche di accountability: la norma definisce l'obiettivo (tutelare i dati personali) e dà alcune regole generali su come raggiungerlo, l'azienda deve decidere/organizzarsi per dimostrare di averlo raggiunto (logica simile al MOG 231/2001)
  - Niente elenchi di misure minime
    Vantaggio: le modalità sono meglio integrabili con i processi di gestione delle aziende «virtuose»
    Svantaggio: le aziende che cercano un elenco di misure minime da implementare per compliance e dimenticarsene, o un po' di «carta da scrivere», non le troveranno
- Valutazione del rischio anche per l'art. 35 (valutazione di impatto):

> 1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura,l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.
> ...
> 7. La valutazione contiene almeno:
> ...
> c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
>
> d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

  - La valutazione del rischio è più affine alle logiche delle aziende e ad es. alla ISO 9001:2015

Problema: valutazione del rischio per gli interessati

Come fa un'azienda a stabilire qual è il rischio adeguato per un soggetto terzo, cioè l'interessato?

Art. 35:

9. **Se del caso**, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

Ma non è una soluzione generale

Possibile strategia: seguire il più possibile le indicazioni dei Garanti (es. CNIL, WP29…), di Agenzie europee (es. ENISA), standard come l'ISO/IEC 29134:2017

Valutazione di impatto

LEVEL OF IMPACT	DESCRIPTION
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Minacce

Di fatto, il riferimento più comune e più ovvio è la ISO/IEC 27001 (e standard collegati)

Feared events	Types of outcomes	Description
Illegitimate access to personal data	None	The data are seen by people who do not need to know them, though these people do not use them.
	Storage	The data are copied and saved to another location without being further used.
	Redistribution	The data are disseminated more than necessary and beyond the control of the data subjects (e.g. unwanted dissemination of a photo on the Internet, loss of control over information published in a social network, etc.)
	Use	The data are used for purposes other than those planned and/or in an unfair manner (e.g. commercial purposes, identity theft, use against data subjects, etc.) or correlated with other information relating to the data subjects (e.g. correlation of residence address and real-time geolocation data, etc.)
Unwanted modification of personal data	Malfunction	The data are modified into valid or invalid data, which will not be used correctly, the processing liable to cause errors, malfunctions, or no longer provide the expected service (e.g. impairing the proper progress of important steps, etc.)
	Use	The data are modified in other valid data, such that the processing operations have been or could be misused (e.g. use to steal identities by changing the relationship between the identity of individuals and the biometric data of other individuals, etc.).
Disappearance of personal data	Malfunction	The data are missing for personal data processings, which generates errors, malfunctions, or provides a different service than the one expected (e.g. some allergies are no longer reported in a medical record, some information contained in tax returns has disappeared, which prevents the calculation of the tax amount, etc.)
	Blockage	The data are missing for personal data processings which can no longer provide the expected service (e.g. slowing down or blocking of administrative or commercial processes, inability to provide care due to the loss of medical records, inability of data subjects to exercise their rights, etc.).

CNIL: «Privacy Impact Assessment Knowledge Bases»

Temi di impatto diretto sul sistema informativo

- «Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita» (Data protection by design e by default, art. 25)
  - Le logiche di protezione dei dati devono entrare nei sistemi e servizi fin dalla progettazione
  - Fondamentale la «data minimization», che non è solo un tema IT
- Tema di grande impatto, soprattutto in prospettiva, è la pervasività della **pseudonimizzazione**
- Procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

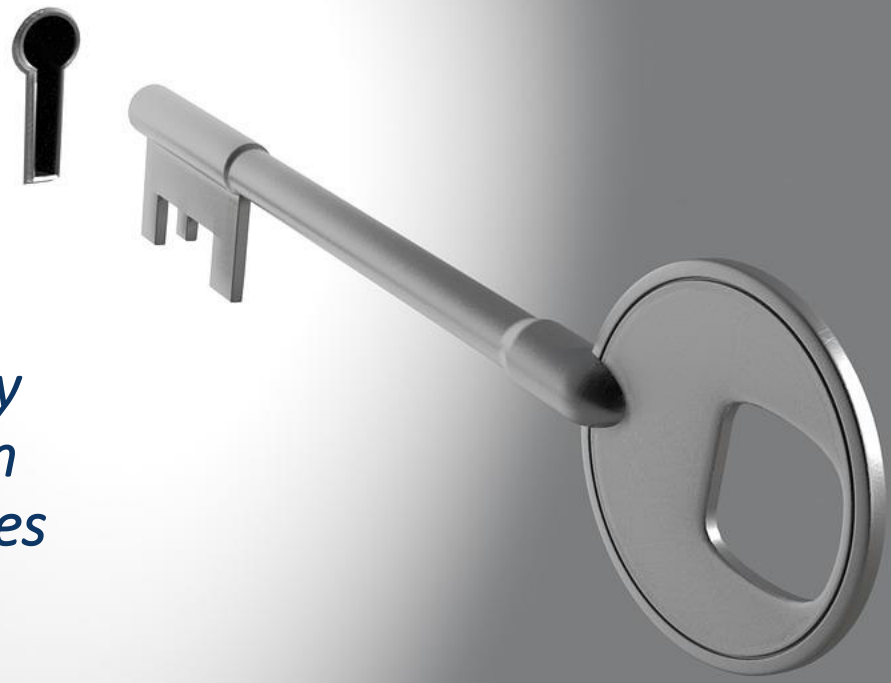
Cifratura obbligatoria?

Nessuna misura di sicurezza è obbligatoria

La cifratura è fortemente suggerita dove è efficace

«Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU»:

Encryption is therefore absolutely necessary and irreplaceable for guaranteeing strong confidentiality and integrity when data are transferred across open networks like the Internet, or stored in mobile devices like smartphones. This encryption should ideally always cover the entire communication, from the device of the sender to that of the recipient (end-to-end-encryption).



Gestione dei data breach

- Notifica di una violazione dei dati personali all'autorità di controllo (art. 33)

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

rilevante per le sanzioni!!

- Comunicazione di una violazione dei dati personali all'interessato (art. 34)

Tutto questo richiede un buon processo di rilevazione e gestione degli incidenti!!

Grazie!

Claudio Telmon
ctelmon@clusit.it