Misure tecniche ed organizzative

(Art. 32, par. 1)

- Pseudonimizzazione.
- Minimizzazione.
- Cifratura.
- Misure specifiche per assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali.

Misure tecniche ed organizzative

- Procedure specifiche per provare, verificare e valutare l’efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento.
- Altre misure specifiche adatte per il trattamento dei dati.
- Sistemi di autenticazione.

Misure tecniche ed organizzative

- Procedure specifiche per provare, verificare e valutare l’efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento.
- Altre misure specifiche adatte per il trattamento dei dati.
- Sistemi di autenticazione.

Misure tecniche ed organizzative

- Sistemi di autorizzazione.
- Sistemi di protezione (antivirus, firewall, antintrusione, altro), adottati per il trattamento dei dati.
- Misure antincendio.
- Sistemi di rilevazione intrusione.
- Sistemi di sorveglianza.

Misure tecniche ed organizzative

- Sistemi di protezione con videosorveglianza.
- Registrazione accessi.
- Porte, armadi e contenitori dotati serrature.
- Sistemi di copiatura e conservazione archivi elettronici.

Misure tecniche ed organizzative

- Altre misure per ripristinare tempestivamente la disponibilità e l’accesso dei dati in caso di incidente fisico o tecnico.
- Procedure per provare, verificare e valutare regolarmente l’efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento

Misure tecniche ed organizzative

- Altre misure per ripristinare tempestivamente la disponibilità e l’accesso dei dati in caso di incidente fisico o tecnico.
- Procedure per provare, verificare e valutare regolarmente l’efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento

LA “*PRIVACY BY DESIGN*”

Principio

Art. 25.1 GDPR

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

Principio

Art. 25.1 GDPR

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 a tutelare i diritti degli interessati”.

In pratica .....

Art. 25.1 GDPR

Il Titolare del trattamento dovrà, fin dalla fase di progettazione, effettuare una valutazione del trattamento dei dati che intende iniziare e dovrà adottare tutte quelle misure e quelli accorgimenti che consentono di operare nel rispetto del regolamento comunitario e delle altre normative di riferimento.

Applicazione

Art. 25.1 GDPR

E’ necessario un coinvolgimento di tutti i soggetti che sviluppano e progettano prodotti, servizi, applicazioni, svolgono attività da cui deriva un trattamento di dati personali.

Applicazione

Art. 25.1 GDPR

I prodotti, i servizi e le attività devono svolgersi, devono essere progettati e sviluppati tenendo conto della normativa in materia di privacy e devono avere caratteristiche tali da permettere ai titolari di adempiere agli obblighi prescritti dalle disposizioni di legge.

Implementazione sistema sicurezza

OBIETTIVO

(Art. 32, par.1)

Devono "***garantire un livello di sicurezza adeguato al rischio***" del trattamento.

Implementazione sistema sicurezza

OBIETTIVO

(Art. 32, par.1)

Lista non esaustiva ma aperta!

Implementazione sistema sicurezza

- E’ necessario dotarsi di un processo di gestione degli “*incidenti di sicurezza*” in quanto un errore potrebbe essere costoso un trattamento illegittimo di dati anche per accesso non autorizzato.

Implementazione sistema sicurezza

- Importante usare tecnologie che permettano l’attivazione di misure di sicurezza e che rilevano immediatamente una qualsiasi violazione.

La formazione

La formazione è una misura di sicurezza per le organizzazioni, **un onere a carico del titolare**, un diritto e dovere per i dipendenti e i collaboratori.

La formazione

La previsione di eventi formativi diretti al personale e ai collaboratori concretizza ***il principio di "accountability"*** **ossia di responsabilizzazione del Titolare del trattamento,** previsto dal Regolamento europeo n. 679/16 **(art.5, par.2)**

La formazione

IMPORTANTE

In ambito pubblico la formazione sulla protezione dei dati non potrà non integrarsi con la digitalizzazione dei processi, con la riforma del CAD, con il Codice di comportamento degli enti e con le disposizioni in materia di trasparenza, prevenzione della corruzione, Foia e whistleblowing.

La formazione

IMPORTANTE

Formazione non come mero adempimento burocratico ma come un’opportunità per rendere consapevoli gli operatori dei rischi connessi al trattamento dei dati, delle misure di sicurezza, per migliorare i processi organizzativi e i servizi erogati, evitare danni reputazionali, ridurre i rischi di sanzioni amministrative.

Pseudonimizzazione

Art. 4.5 GDPR

«il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile» .

Pseudonimizzazione

Considerando 28 GDPR

«L’applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati».

Pseudonimizzazione

E’ un processo mediante il quale i dati sono conservati in un formato che non identifichi direttamente un individuo specifico senza l’utilizzo di informazioni aggiuntive.

Pseudonimizzazione

Consente di raccogliere dati diversi ma relativi allo stesso soggetto, senza che di esso si conosca l’identità in modo diretto.

Pseudonimizzazione

Anche se il soggetto rimane identificabile, devono comunque sussistere motivi legittimi per effettuare la reidentificazione in quanto i dati personali devono essere ***«raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità»*** (Art. 5.1.b), GDPR).

Pseudonimizzazione

Implica tre elementi

- l’assenza di identificabilità diretta del soggetto interessato (***«trattamento dei dati personali in modo tale che i dati non possano essere più attribuiti ad un interessato specifico senza l’utilizzo di informazioni aggiuntive»***)

Pseudonimizzazione

- l’adozione di misure di sicurezza ulteriori da aggiungere alla pseudonimizzazione (***«a condizione che tali informazioni aggiuntive siano conservate separatamente»***);

Pseudonimizzazione

- l’incorporazione della pseudonimizzazione nella privacy-by-design («e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile»).

Pseudonimizzazione

Il valore della pseudonimizzazione sta nel non essere solo una tecnica da combinarsi con ulteriori misure di sicurezza, ma nell’avere un efficacia che consente di considerarla già di per sé una misura adottata a tutela dei dati personali dei soggetti interessati, per diminuirne i rischi di identificazione diretta.

Pseudonimizzazione

IMPORTANTE

Sia la pseudonimizzazione che l'anonimizzazione vengono poste a tutela del singolo individuo, inteso come "soggetto identificabile", al fine di garantirgli protezione rispetto alle attività di profilazione mirate che comportano l'identificazione del soggetto (*single out*).

Es. di Pseudonimizzazione

Pseudonimizzazione dei dati di Mario Rossi

- Si attribuisce alla scheda di Mario Rossi un **codice identificativo univoco**;

- Si crea una **tabella separata** in cui quel codice è abbinato a tutte le informazioni che possono condurre all'identificazione alla persona, come nome, email, numero di telefono, codice fiscale eccetera;

Es. di Pseudonimizzazione

- Si **eliminano dalla scheda dei dati pseudonimizzati i dati identificativi** di Mario Rossi lasciando solo il codice identificativo come mezzo per ricollegare le due tabelle.