LA “*RESPONSABILIZZAZIONE*”

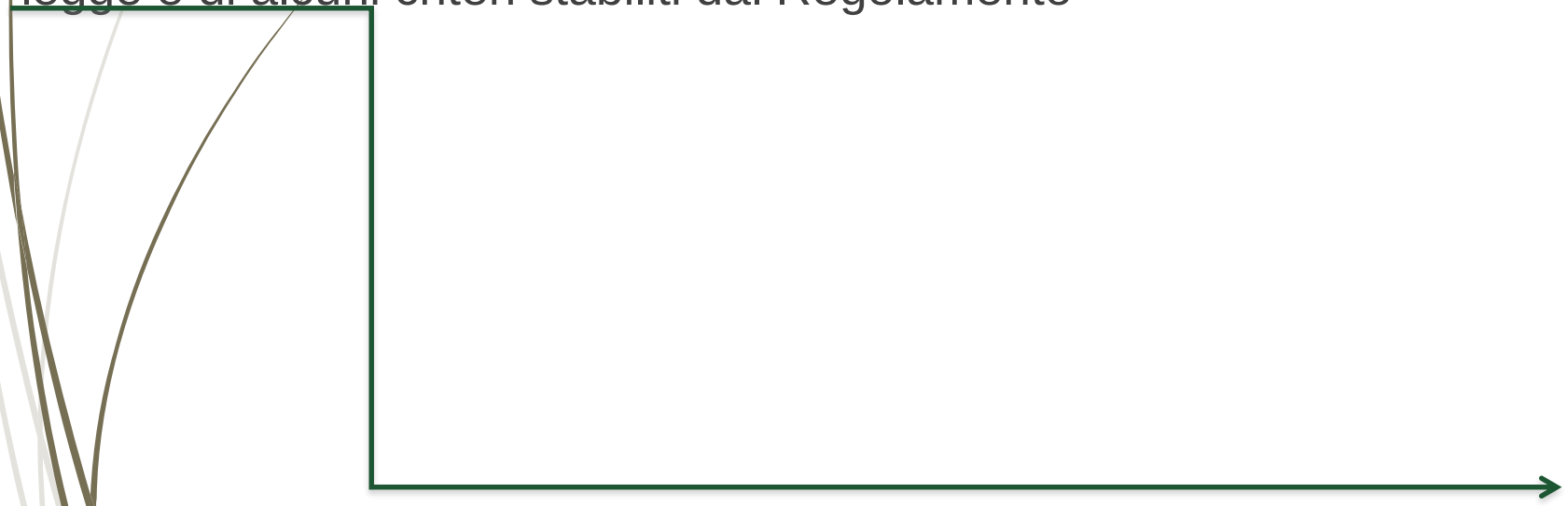
Cosa è?

Una novità importante è l'introduzione del principio di "*responsabilizzazione*" ("*accountability*") del titolare del trattamento dei dati.

Adozione di comportamenti tali da dimostrare la concreta adozione di misure idonee per l'applicazione del Regolamento (**Artt . 23-25 e Capo V**)

Chi?

E’ affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto della legge e di alcuni criteri stabiliti dal Regolamento



I criteri

CRITERI

- **“*data protection by default and by design*” (Art. 25 Reg.)**

  Consiste nella configurazione del trattamento prevedendo sin dall’inizio le garanzie indispensabili “***al fine di soddisfare i requisiti***” del Reg. e tutelare i diritti degli interessati.

I criteri

CRITERI

- **Rischio inerente il trattamento (Considerando 75-77)**

E’ il rischio di produrre impatti negativi sulle libertà e sui diritti degli interessati

analizzati mediante processo di valutazione (Artt.35-36) tenendo conto dei rischi noti e delle misure tecniche ed organizzative che il titolare deve adottare.

I criteri

CRITERI

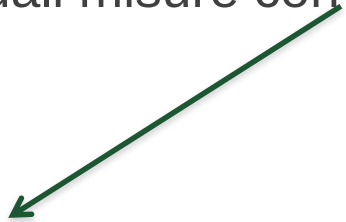
- **Rischio inerente il trattamento (Considerando 75-77)**

Dopo la valutazione il titolare decide se iniziare il trattamento o se chiedere indicazioni al Garante Privacy il quale può indicare ulteriori misure di sicurezza che il titolare deve implementare .....

I criteri

CRITERI

- ma potrà anche adottare le eventuali misure correttive (Art. 58)



- Ammonimento titolare, limitazione trattamento , divieto di procedere al trattamento.

I criteri

Conseguenza.....

abolizione dal 25 maggio della notifica preventiva dei trattamenti al Garante e del c.d. prior checking o verifica preliminare (art. 17 Codice) sostituiti da:

- Obblighi di tenuta del registro del trattamento.
- Effettuazione valutazione di impatto dei rischi.

GLI STRUMENTI

Gli strumenti

- Registro delle attività di trattamento.
- Registro delle categoria di attività
- Valutazione di impatto sulla protezione dei dati.

Registro attività di trattamento

Costituisce “*il libro mastro*” del Sistema *Privacy*, cioè il punto di partenza per la predisposizione dell’intero impianto documentale e raccoglierà le evidenze, i controlli e i processi che portano a soddisfare l’”accountability” del Sistema *Privacy*.

Registro attività di trattamento

Contenuto (Art. 30)

- Il nome e di dati di contatto dell'Ente del RPD;
- Le finalità del trattamento;
- La descrizione in modo sintetico delle categorie dei soggetti interessati e le categorie dei dati personali.

Registro attività di trattamento

Contenuto (Art. 30)

- Categorie dei destinatari ai quali i dati sono stati o saranno comunicati.
- Eventuale trasferimento di dati personali verso un paese terzo od organizzazione internazionale.

Registro attività di trattamento

Contenuto (Art. 30)

- I termini per la cancellazione delle categorie dei dati, se previsti.
- Le misure di sicurezza tecniche ed organizzative che sono state adottate.

Registro attività di trattamento

Contenuto (Art. 30)

- Sostanziale coincidenza fra i contenuti della notifica dei trattamenti (art. 38 Codice) e quelli ex art. 30 Regolamento.

Registro attività di trattamento

Forma

- Deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta del Garante Privacy.

Registro categorie di trattamento

Contenuto

- Nome e dati di contatto del RTD e RPD;
- Le categorie di trattamento effettuate da ogni Responsabile.
- L’eventuale trasferimento dei dati personali verso un Paese terzo od organizzazione internazionale;
- Le misure di sicurezza tecniche ed organizzative adottate.

Registro categorie di trattamento

Contenuto

- Nome e dati di contatto del RTD e RPD;
- Le categorie di trattamento effettuate da ogni Responsabile.
- L'eventuale trasferimento dei dati personali verso un Paese terzo od organizzazione internazionale;
- Le misure di sicurezza tecniche ed organizzative adottate.

Registro categorie di trattamento

IMPORTANTE

Se un trattamento possa presentare un rischio elevato per i diritti e le libertà personali, il Titolare, prima di effettuare il trattamento deve effettuare una VIPD (art. 35 RGPD).

Valutazione impatto protezione dati (DPIA)

Art. 35 RGPD

E’ una procedura che ha come scopo di:

- di descrivere il trattamento al fine di valutare la sua necessità e la proporzionalità.
- facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali.

Valutazione impatto protezione dati (DPIA)

Art. 35 RGPD

E’ una procedura che ha come scopo di:

- di permettere la realizzazione e la dimostrazione che il trattamento dei dati è conforme alla legge.

Valutazione impatto protezione dati (DPIA)

IMPORTANTE

Linee guida in materia di valutazione di impatto in

http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

IL *DATA BREACH*

Definizione

Evento in conseguenza del quale si verifica una
“violazione dei dati personali”.

E’ un incidente di sicurezza in cui dati personali, sensibili, protetti o riservati sono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato anche a seguito di un evento accidentale.

Tipologia

La casistica è molto estesa, un “*data breach*” si può anche verificare seguito di un problema *hardware* o *software* o con una divulgazione di dati riservati o confidenziali all’interno di un ambiente privo di misure di sicurezze (da es. su web) in maniera involontaria o volontaria o con il furto di dati ecc.…

Tipologia

- Data Exfiltration
- Ransomware/Malware
- Distruzione accidentale archivio digitale
- Smarrimento/ Furto PC/Server
- Smarrimento/furto dispositivo mobile(USB KEY, CD/DVD HD, etc.
- Distruzione archivio cartaceo
- Smarrimento/furto archivio cartaceo

Come faccio a saperlo?

- Segnalazione del CED interno
- Chiamata del fornitore esterno
- Segnalazione della polizia postale
- Segnalazione da AGID
- Segnalazione dell’interessato
- Comunicazione su Internet/Stampa
- etc.

I potenziali soggetti coinvolti

- Sindaco
- Segretario Comunale
- DPO
- Responsabile Trattamento Dati
- Responsabile URP
- Responsabile del Personale
- Responsabile Ufficio Legale

I potenziali soggetti coinvolti

- Ufficio /Consulente privacy
- Amministratore di sistema
- Polizia Postale
- Garante Privacy
- Interessati
- Etc….

I potenziali soggetti coinvolti

TORI	FASE 1: Rilevazione	FASE 2: gestione Tecnica e Analisi	FASE 3: raccolta informazioni e invio notifica al Garante	FASE 4: comunicazioni interessati e riscontri	FASE 5: Registrazione della violazione
daco		X	X		
gretario Comunale		X			
O	X	X	X	X	X
sponsabile Trattamento Dati erno	X	X			
igente Interno delegato		x	x		
sponsabile URP				X	
sponsabile del Personale		X			
sponsabile Ufficio Legale o nsulente legale			X		x
sponsabile Ufficio Privacy o nsulente privacy		X			
lizia Postale	x	X			
rante				x	
eressati				X	

Obbligo comunicazione

L’art. 33 GDPR impone al titolare del trattamento di notificare al Garante Privacy la violazione di dati personali entro 72 ore dal momento in cui il titolare ne viene a conoscenza.

Obbligo comunicazione

Termine non perentorio ma in caso di superamento deve essere data giustificazione al Garante, dei motivi del ritardo, unitamente alla notifica.

Non - Obbligo comunicazione

(Art. 33, par. 1)

Notifica non necessaria quando il titolare ritiene che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Sanzioni

Art. 58 GDPR

In caso di mancato rispetto dell'obbligo di notifica, Garante applica misure correttive:

- avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere i flussi dati.

Sanzioni

Art. 83 GDPR

In caso di mancato rispetto dell'obbligo di notifica, Garante impone sanzioni amministrative:

- **Fino a €. 10.000.000.**