

GDPR

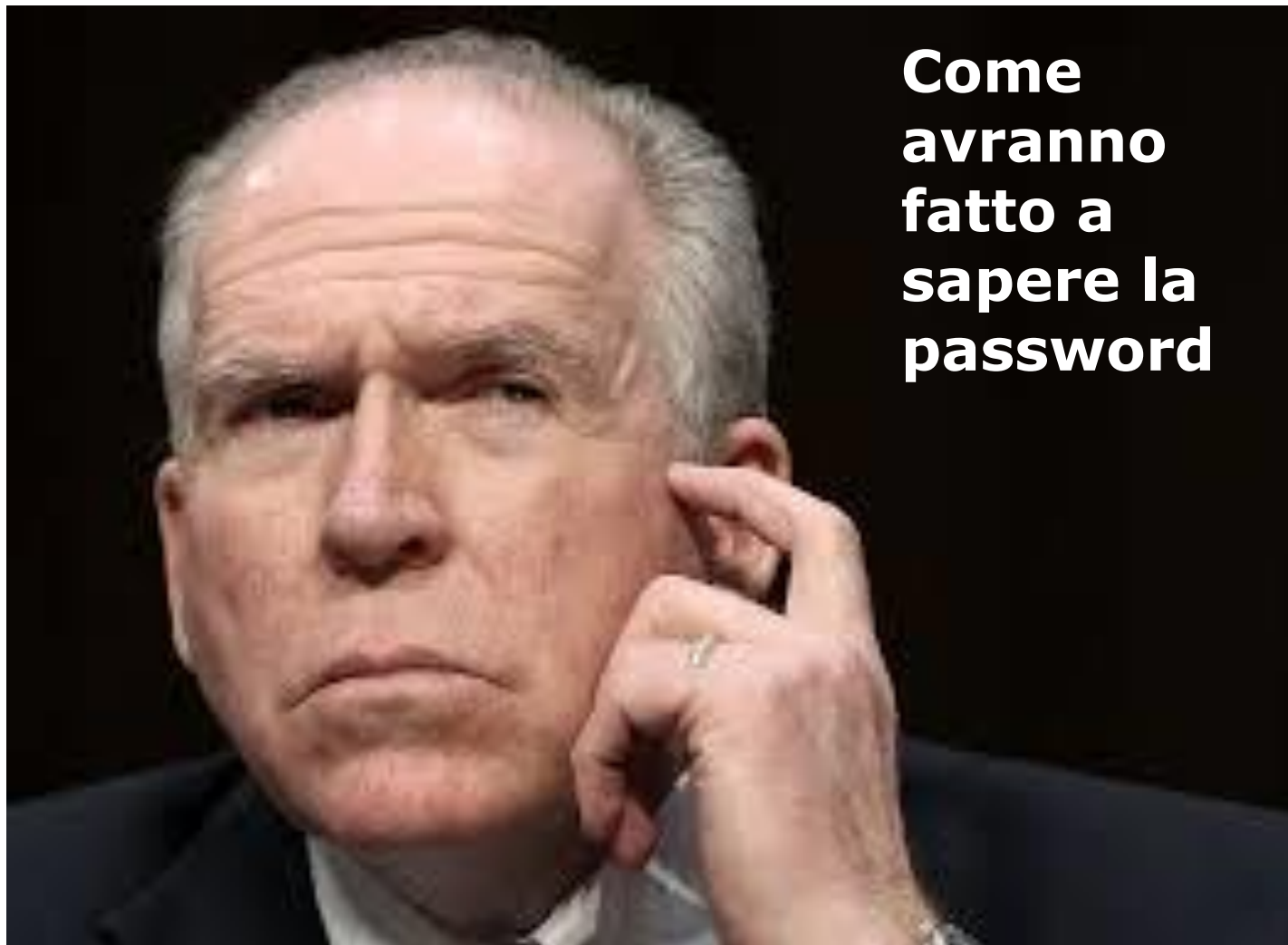
Istruzioni per l'uso e la rivoluzione dell'accountability

Approccio basato sul rischio e misure di
responsabilizzazione dei titolari e responsabili

Il caso Facebook



Violazione del dato: le mail



Obiettivi e contenuti – la domanda



- **La privacy è semplice rispetto della legge o integrità nel business, gestione del rischio o quality marketing?**
- **Rispondere è l'obiettivo dell'incontro:** partiremo dal fornire le prime informazioni sul Regolamento Europeo in materia di protezione dei dati e poi affronteremo il concetto della accountability (che sarà la chiave di lettura di tutto ciò che faremo).

Regolamento europeo - GDPR



25 gennaio 2012: la Commissione Europea presenta una serie di proposte per le modifiche al quadro giuridico in materia di protezione dei dati.

12 marzo 2014: approvazione della versione definitiva (o quasi) del Regolamento.

15 dicembre 2015: trovato l'accordo sulla riforma della normativa sul trattamento dei dati personali.

5 maggio 2016: approvato il 679/2016 e pubblicato in Gazzetta Ufficiale il Regolamento Europeo.

25 maggio 2018: entrata in vigore.

La Privacy oggi

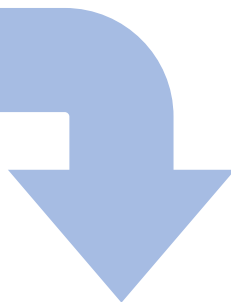


GDPR PUNTI PRINCIPALI



- **Informativa:** articolo 13 - estesa e dettagliata.
- **Consenso:** il titolare deve essere in grado di dimostrare che ci sia il consenso a uno specifico trattamento.
- **DPO.**
- **Registro dei trattamenti:** strumento operativo per una corretta gestione dei dati.
- **Valutazione dei rischi (DPIA).**
- *Privacy by design.*

Le principali novità



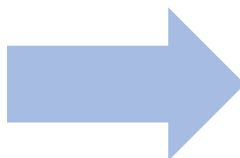
- Obbligo per gli enti pubblici e per le **aziende**, che trattano dati particolarmente critici o sensibili, di nominare un "**Data Protection Officer**" (responsabile della protezione dei dati personali), che dovrà essere competente, indipendente e non necessariamente interno all'ente/impresa.
- Obbligo di "**privacy impact assessment**" (PIA - valutazioni preventive di impatto sulla tutela dei dati in caso di trattamenti rischiosi).
- **Adozione di misure di sicurezza** coerenti con la PIA e con i trattamenti effettuati.
- Creazione dei **registri dei trattamenti**: il titolare e il responsabile del trattamento devono redigere i registri di competenze in cui indicare le **caratteristiche, modalità e finalità dei trattamenti**. Obbligo limitato ad alcuni casi specifici.

DPO: nomina



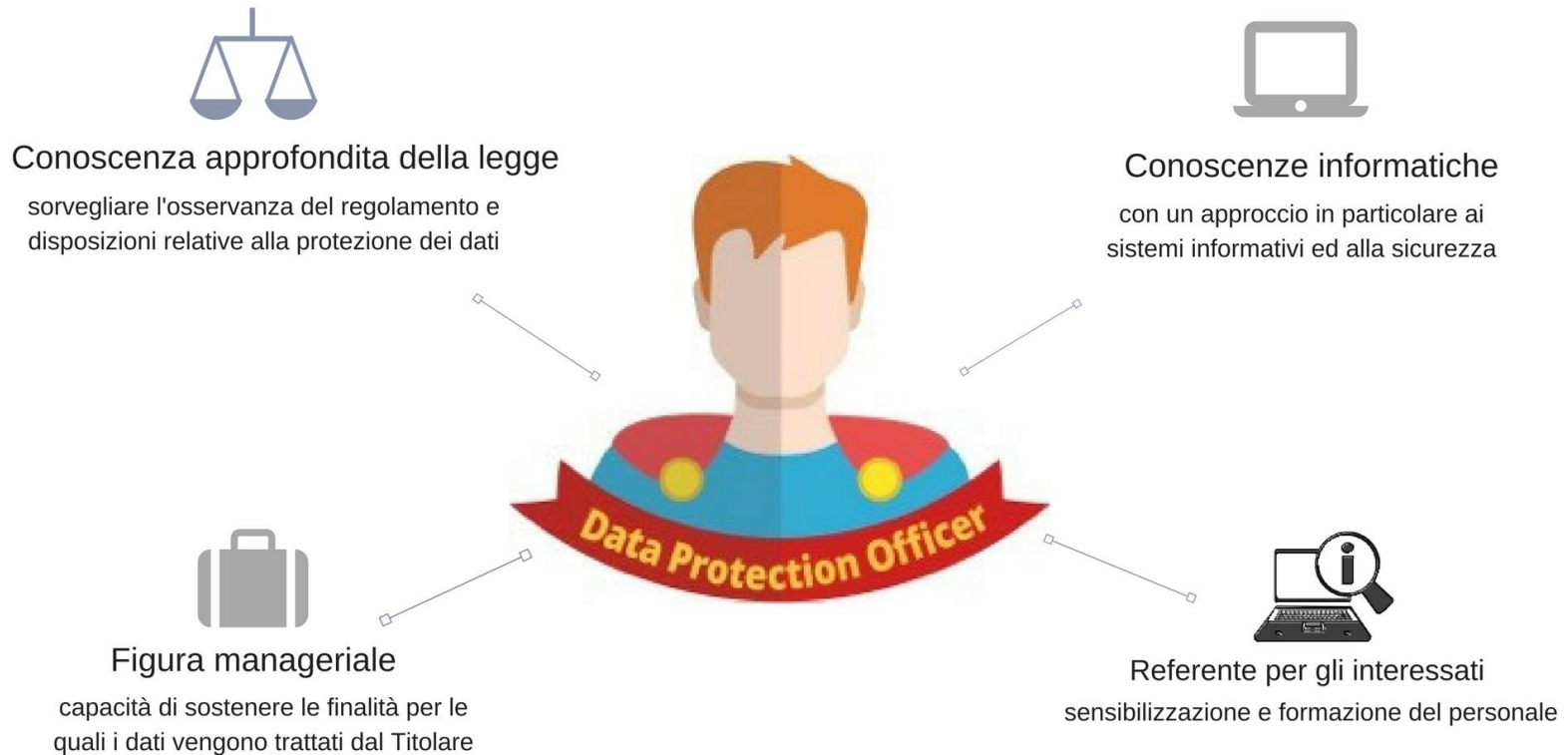
contratto di servizi stipulato con una persona fisica o giuridica esterna all'organismo o all'azienda dal titolare/responsabile del trattamento

Quando è obbligatorio



- Enti pubblici e società partecipate da enti pubblici.
- Nel caso di trattamento di categorie particolari di dati sensibili in modo sistematico.
- Monitoraggio sistematico su larga scala.

Competenze del DPO



Punto di contatto per: **interessati - autorità di controllo - soggetti interni all'organismo o all'ente**

Registro dei trattamenti



- Tenere traccia delle operazioni di trattamento effettuate all'interno di un'azienda.
- Strumento operativo di lavoro mediante il quale censire in maniera ordinata le banche dati.
- In forma scritta, anche elettronica.

Parte integrante di un sistema di corretta gestione dei dati personali, indispensabile per ogni valutazione e analisi del rischio.

Valutazione dei rischi - DPIA

Articolo 35: Valutazione di impatto sulla protezione dei dati

Procedura che permette di dimostrare la conformità alle norme in materia di protezione dei dati personali.

Gli **obiettivi** della Data Protection Impact Assessment:

- descrivere il trattamento,
- facilitare, attraverso misure idonee, la gestione dei rischi che potrebbero minare i diritti e le libertà delle persone fisiche per le quali viene effettuato il trattamento.

Operazione obbligatoria in tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche

Le misure di sicurezza

Non più misure "minime" di sicurezza.



Titolare e Responsabile devono "garantire un livello di sicurezza adeguato al rischio, attraverso misure tecniche e organizzative quali:

- cifratura dei dati personali,
- codici di condotta/schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza".

La rivoluzione dell'*accountability*



Principio per il quale ogni titolare, in caso di problemi o controlli, dovrà dimostrare nei fatti, al di là dei formalismi, di avere adottato i modelli organizzativi e le misure **logiche, fisiche, elettroniche** di sicurezza per proteggere i dati (onere della prova) – questo porterà a dover creare un sistema documentale di gestione della privacy.

Significa capacità di rendere conto, saper dimostrare.

Privacy by design



Al principio dell'accountability si collega quello di *"data protection by design & by default"*:

Tenendo conto del contesto complessivo del trattamento e dei rischi per i diritti degli interessati, responsabile e titolare dovranno adottare, prima del trattamento stesso, garanzie indispensabili al fine di soddisfare i requisiti del regolamento. **Il sistema deve porre al centro la sicurezza dei dati dell'utente.**

Conclusioni

Le principali attività di adeguamento



Gap Analysis



Registro dei trattamenti



Valutazione dei rischi



Informative

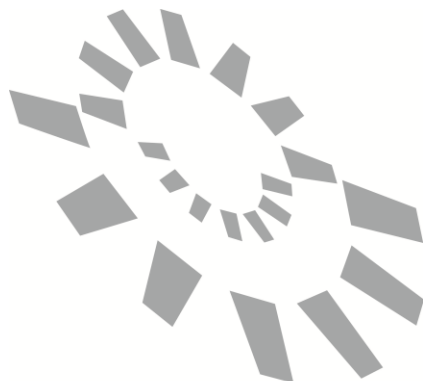


Procedure



Monitoraggio

Fonte infografica: Audit in Italy S.r.l.



ICIM

Certifichiamo oggi
per il domani.

**Grazie
per l'attenzione**

www.icim.it



ICIM S.p.A.
Piazza Don Mapelli, 75
20099 Sesto San Giovanni (MI) – Italy
Tel. +39 02 725341
Fax. +39 02 72002098
www.icim.it

