ACCOUNTABILITY, SICUREZZA E DATA BREACH

Avv. Sergio Falcone

Coordinatore Commissione Privacy & Security
del COA di Napoli

«BIGGER RESPONSIBILITIES, BIGGER REPERCUSSIONS»

ACCOUNTABILITY, RISK ANALYSIS AND DATA BREACH: HOW TO ACHIEVE A PRIVACY COMPLIANCE TO GDPR

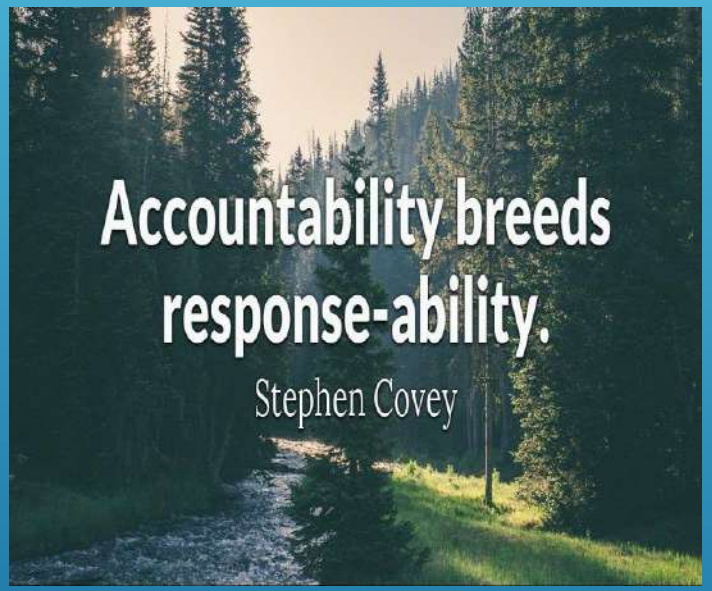
GDPR: IL NUOVO RISK BASED APPROACH

2010

2019

Il termine inglese "**accountability**" (**responsabilità**) viene utilizzato nel mondo anglosassone in contesti specifici, pressoché finanziari. E' senza dubbio arduo tradurre univocamente il termine. Da un punto di vista lessicale nasce come parola composta dall'unione del verbo *to account*, traducibile in italiano come "**dar conto**", ed il sostantivo "ability" che significa "**essere in grado di".**

Il concetto di "**responsibility**" è legato ad un'azione concreta, al «**fare**».
Il concetto di "**accountability**" è legato al «**rendere conto**» dell'azione fatta o fatta fare.
Nonostante la evidente differenza non solo formale bensì concettuale, in italiano entrambi vengono tradotti con un unico termine: **responsabilità**.



Il principio di **accountability** richiama dunque sia ad un **obbligo di responsabilizzazione** che ad un **obbligo di rendicontazione**: il titolare del trattamento, infatti, non solo deve adottare misure tecniche, organizzative e legali idonee a garantire una adeguata ed efficace protezione dei dati personali, anche attraverso lo studio di modelli organizzativi ad hoc, ma ha anche l'onere di documentare e dimostrare che il trattamento dei dati sia stato effettuato in conformità al Regolamento Europeo in materia di privacy.

Articolo 5

Principi applicabili al trattamento di dati personali

«**1.** I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («**liceità, correttezza e trasparenza**»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («**limitazione della finalità**»);

L'ACCOUNTABILITY NEL TESTO NORMATIVO EUROPEO

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («**esattezza**»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; .....

L'ACCOUNTABILITY NEL TESTO NORMATIVO EUROPEO

…i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («**limitazione della conservazione**»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («**integrità e riservatezza**»).

L'ACCOUNTABILITY NEL TESTO NORMATIVO EUROPEO

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo».

L'ACCOUNTABILITY NEL TESTO NORMATIVO EUROPEO

L'Autorità garante francese ha multato **Google** per un totale di **50 milioni di euro** per aver infranto il GDPR. La motivazione riportata sulla sanzione è stata «**mancanza di trasparenza, informazioni adeguate e mancanza di un valido consenso In merito alla personalizzazione degli annunci**».

« Le informazioni rilevanti sono accessibili solo dopo diversi passaggi, il che implica talvolta fino a 5 o 6 azioni» e quindi «gli utenti non sono in grado di comprendere appieno l'entità delle operazioni di elaborazione eseguite da Google». L'importo deciso e la pubblicità dell'ammenda sono giustificati, secondo la Commissione d'Oltralpe, dalla gravità delle violazioni osservate riguardo ai principi essenziali del Regolamento europeo: **trasparenza, informazione e consenso**.

VIOLAZIONE GDPR: IL CASO GOOGLE

Articolo 24

Responsabilità del titolare del trattamento

«**1.** Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, **il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento**. Dette misure sono riesaminate e aggiornate qualora necessario.

L'ACCOUNTABILITY NEL TESTO NORMATIVO EUROPEO

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono **l'attuazione di politiche adeguate in materia di protezione dei dati** da parte del titolare del trattamento.
3. L'adesione ai **codici di condotta** di cui all'articolo 40 o a un **meccanismo di certificazione** di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento».

L'ACCOUNTABILITY NEL TESTO NORMATIVO EUROPEO

Il GDPR obbliga quindi, in chiave di accountability, titolari e responsabili ad **adottare comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento**.

Si tratta di una **grande novità per la protezione dei dati** poiché viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative dettate dal GDPR stesso.

GDPR: APPROCCIO PROATTIVO ALLA PRIVACY MANAGEMENT

Privacy by design, riguarda il principio di incorporazione della privacy a partire dalla progettazione di un processo aziendale con le relative applicazioni informatiche di supporto. Questo implica la messa in atto di determinati meccanismi che garantiscono il trattamento esclusivo di dati personali necessari per quella specifica progettazione.

Privacy by default, si traduce con la necessità di tutelare la vita privata dei cittadini ***di default***, ovvero come **impostazione predefinita** dell'organizzazione aziendale, chiamata a trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti, in modo che l'interessato riceva un alto livello di protezione anche se non si attiva per limitare la raccolta dei dati.

Accountability ☞

Risk analysis ☞

Data breach ☞

«Affermare di aver raggiunto la piena conformità perché è stato completato un progetto di adeguamento senza che questo venisse accompagnato dalla ***definizione di un sistema di gestione interno della privacy*** *è come provare a fare una foto a un treno in corsa…(CIT.)»*

L'approccio proattivo alla privacy management stabilito dal Legislatore europeo conferisce un ruolo chiave allo strumento della **risk analysis**, chiamato a dimostrare l'adeguatezza delle misure implementate dal titolare a tutela dei dati oggetto del trattamento, e a riprova del principio di **accountability.**

LA RISK ANALYSIS NEL GDPR

*La **privacy management** deve mirare al raggiungimento di una piena **compliance** al dettato normativo, possibile solo attraverso la creazione di un **sistema di gestione tailored fit, studiato ad hoc ed ex ante** sulla base delle caratteristiche peculiari dell'organizzazione e sui trattamenti di dati personali che intenderà svolgere.*

Fasi per la creazione di una idonea privacy management in chiave di compliance:

1 –  **creazione di un modello ad hoc di gestione della privacy**

2 –  **mappatura di tutti i trattamenti dei dati personali effettuati**

3-  **implementazione delle attività di verifica e controllo**

1- DEFINIZIONE DI UN MODELLO PRIVACY

- definizione **del contesto e di tutti i soggetti coinvolti** in chiave attiva e passiva nel trattamento dei dati
- definizione e condivisione **dei sistemi di sicurezza** prescelti con tutti i soggetti chiamati al trattamento dei dati
- definizione **di procedure di verifica** dell'applicazione e del rispetto dei sistemi di sicurezza adottati
- definizione **di percorsi formativi** per il personale coinvolto nel trattamento dei dati

2- MAPPATURA DEI TRATTAMENTI

- creazione di un **registro dei trattamenti** in cui riportare tutti i trattamenti effettuati dall'organizzazione
- compilazione del registro attraverso la raccolta dei dati personali

Affinchè si realizzi la privacy compliance occorre procedere con una verifica periodica del rispetto delle misure di sicurezza previste per scongiurare una possibile violazione dei dati personali trattati. Ciò si traduce nella **risk analysis** supportata da una **DPIA** (Data Protection Impact Assessment) laddove prevista.

PRIVACY COMPLIANCE

3- IMPLEMENTAZIONE DI ATTIVITA' DI VERIFICA

- verifica e aggiornamento periodici delle **informative privacy** e del **sito** istituzionale dell'organizzazione
- predisposizione di un **data breach management**, attraverso la creazione di strumenti idonei all'individuazione di un eventuale incidente e la valutazione sulla presenza di **violazione di dati personali**. Predisposizione di una procedura che preveda la notifica all'Autorità garante, ed eventualmente agli interessati. Predisposizione e tenuta di un data breach register.

La gestione dei rischi in ambito privacy si traduce dunque nell'insieme di tutte le attività volte ad indirizzare e controllare un'organizzazione in relazione ai rischi sui trattamenti dei dati personali.

Il Regolamento richiama il **risk management** attraverso due modalità:

1 – una **valutazione dei rischi per i diritti e le libertà delle persone fisiche** ex artt. 24, 25 e 32 GDPR

2 – una **valutazione di impatto sulla protezione dei dati (DPIA)** ex art. 35 GDPR

RISK MANAGEMENT

Il **risk management** permette di prevenire, e quindi evitare la possibilità di violazione dei dati personali oggetto di trattamento all'interno dell'organizzazione. Sintetizzando e semplificando tale insieme di operazioni, potremmo definire ex ante **3 fasi**:

1 –  la **previsione** dei possibili eventi negativi

2 –  la **progettazione e realizzazione** di un piano di sicurezza

3 – 

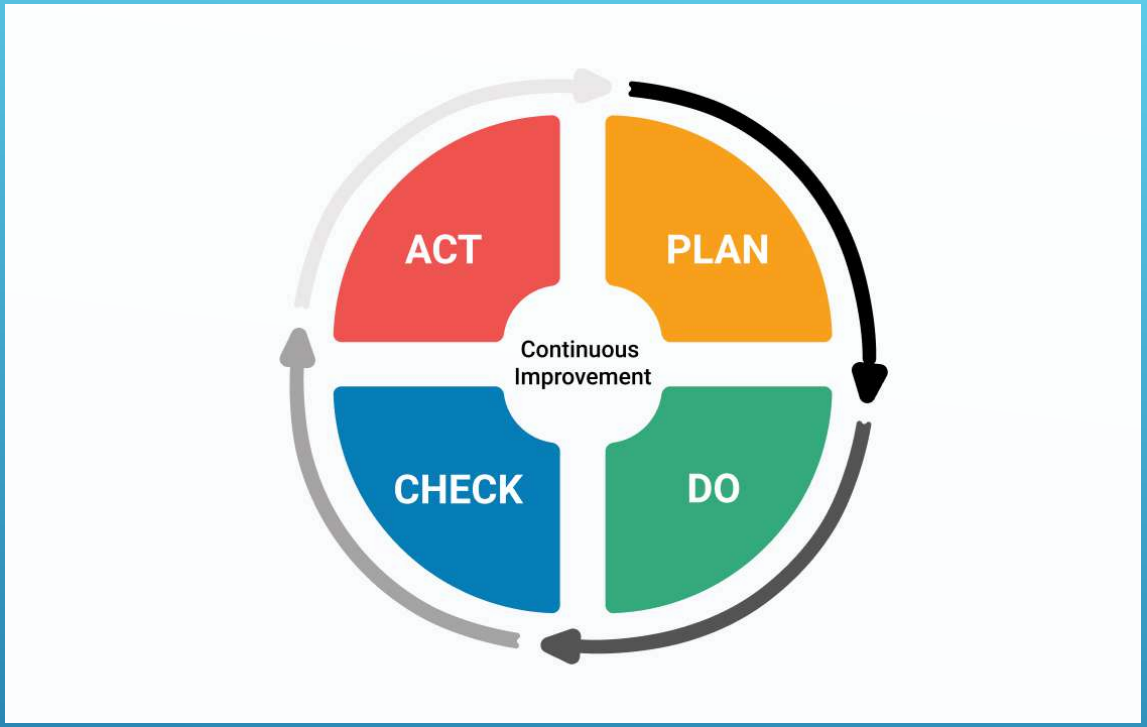
la **valutazione** del piano elaborato

RISK MANAGEMENT

- **IDENTIFICAZIONE DEI RISCHI**
- **SCELTA ED ESECUZIONE DEGLI INTERVENTI**
- **VALUTAZIONE DEGLI INTERVENTI**

Le 3 fasi del risk management si collocano all'interno di un **processo dinamico di tipo circolare**: laddove l'individuazione e la successiva valutazione sull'efficacia degli interventi dovesse risultare negativa, si dovrà tornare ad una nuova e più esaustiva identificazione e quantificazione dei rischi, e quindi alla progettazione di nuove e più efficaci strategie.

RISK MANAGEMENT



PIANIFICAZIONE
= progettazione del sistema di sicurezza privacy

IMPLEMENTAZIONE
= creazione del sistema progettato

VERIFICA
= controllo dell'efficacia delle misure adottate

MESSA IN ATTO
= adozione del sistema

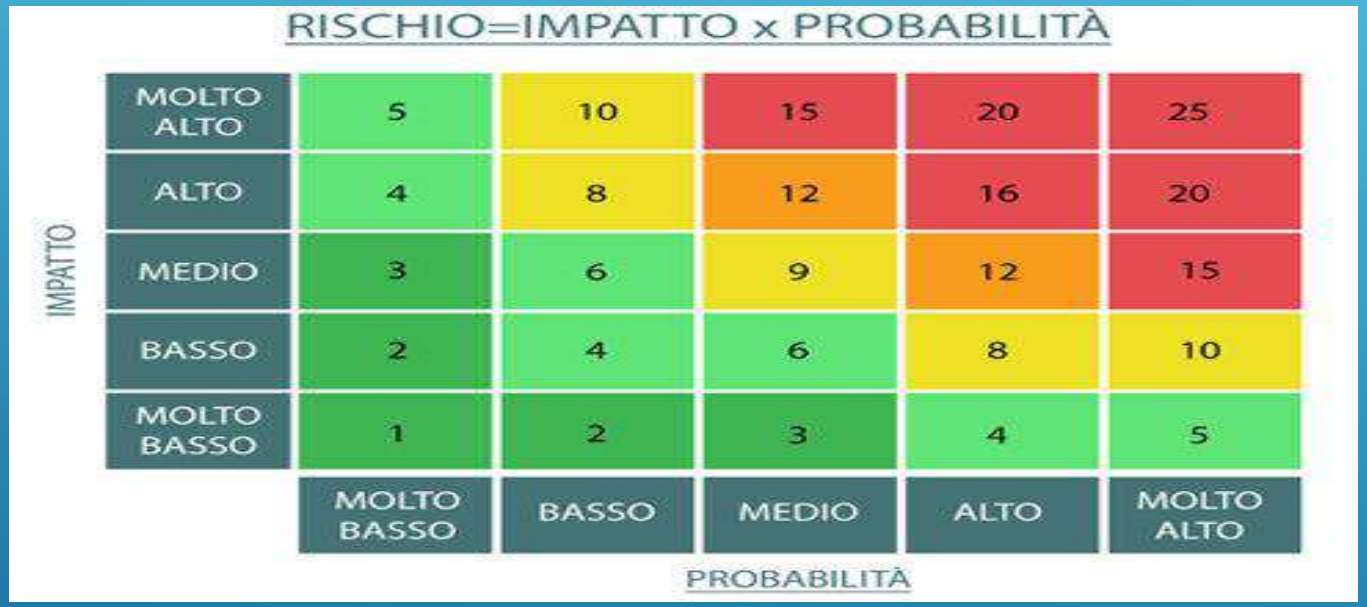
circolarità fasi → **adeguamento** → **privacy management improvement**

RISK ANALYSIS E PDCA CYCLE

Ai fini di una corretta ed idonea risk analysis riveste un ruolo centrale la **scelta della modalità di valutazione, e quindi classificazione dei rischi**. In tale contesto il GDPR non fornisce indicazioni specifiche, risulta pertanto determinante attingere **modelli di valutazione dei rischi dalle linee guida e dalle raccomandazioni del Garante per la Privacy, del WP29, o da fonti autorevoli quali agenzie e organismi di certificazione.**

RISK ANALYS

I rischi connessi al trattamento di dati personali devono necessariamente essere valorizzati, quantificati. A tal fine ciascuna organizzazione può liberamente avvalersi di un proprio **modello** per categorizzare e misurare i rischi, oppure attingere a modelli qualitativi, quantitativi o misti largamente presenti in letteratura. La **matrice per il calcolo del rischio potenziale lordo** rappresenta il modello di riferimento per la misurazione del rischio in ambito privacy.



RISK ANALYS E MATRICE PER IL CALCOLO DEL RISCHIO

Il **registro dei trattamenti** permette di disporre di un **quadro aggiornato dei trattamenti** posti in essere all'interno dell'organizzazione. Attraverso la redazione e l'aggiornamento del registro è possibile quindi impostare fin dalle prime fasi un adeguato approccio alla sicurezza, non tralasciando l'altra importante funzione del registro, ossia quella di **dimostrazione della conformità della gestione privacy** dell'organizzazione ai dettati del GDPR in caso di verifica da parte dell'Autorità di controllo .

RISK MANAGEMENT E REGISTRO DEI TRATTAMENTI

Il garante della privacy ha sanzionato con una multa di € 50.000,00 la piattaforma Rousseau poiché «***non garantisce la protezione delle schede elettroniche e l'anonimato dei votanti in tutte le fasi del procedimento elettorale elettronico***". Dunque, "*non gode delle proprietà richieste a un sistema di e-voting*»

Tra le principali criticità evidenziate, il fatto che gli **amministratori detengono una password unica** e possono entrare nella piattaforma senza lasciare traccia, dunque con un **margine di manipolazione potenzialmente molto alto**. Inoltre, alcuni database consultabili contengono le informazioni relative alle operazioni di e-voting dei periodi precedenti, con un ID utente che permette indirettamente di **risalire al soggetto votante.**

VIOLAZIONE GDPR: IL CASO ROUSSEAU

La DPIA si configura come un **processo in grado di valutare la liceità, necessità e proporzionalità del trattamento, e di valutare e gestire i rischi per i diritti e le libertà delle persone fisiche i cui dati personali sono trattati**. Laddove un trattamento evidenzi la possibilità di un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare ha difatti l'obbligo di effettuare una **DPIA (Data Protection Impact Assessment**

RISK MANAGEMENT E DPIA

La DPIA è **richiesta** nello specifico (art. 35, par. 3 GDPR):

- laddove si proceda ad una "**valutazione sistematica e globale** di aspetti personali relativi a persone fisiche, basate **su un trattamento automatizzato**, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche";
- nel caso di "**trattamento, su larga scala, di categorie particolari di cui all'articolo 9, paragrafo 1, o i dati relativi a condanne penali e ai reati di cui all'art. 10**" (cd. dati sensibili e dati relativi a condanne penali e reati);
- nel caso di "**sorveglianza sistematica su larga scala** di una zona accessibile al pubblico".

Il GDPR non fornisce criteri per addivenire alla quantificazione numerica della cd. «**larga scala**». Il WP29 raccomanda di tenere in considerazione i seguenti fattori per determinare se il trattamento venga effettuato o meno su larga scala:

- **Il numero di interessati** – come numero specifico o come percentuale della popolazione pertinente
- **Il volume di dati**/o il range dei diversi dati in elaborazione
- **La durata**, o permanenza, dell'attività di elaborazione dei dati
- **L'estensione geografica** dell'attività di elaborazione

Il WP29, intervenuto per integrare la normativa europea, ritiene invece che la **DPIA non** sia **richiesta** nei seguenti casi:

- laddove **il trattamento non presenti un "rischio elevato** per i diritti e le libertà delle persone fisiche"

- laddove le caratteristiche di un trattamento (contesto, finalità, natura ed ambito di applicazione) siano del tutto simili a quelle di un **trattamento per il quale è già stata effettuata una DPIA**

RISK MANAGEMENT E DPIA

Riassumendo:

- **la DPIA, per la parte relativa alla risk analysis su un trattamento, va eseguita sempre prima che questo abbia inizio**

- **l'analisi va effettuata su ciascun singolo trattamento, salvo il caso di trattamenti simili**

Per quanto concerne le **misure tecniche** da adottare laddove, all'esito dell'analisi svolta nell'ambito della DPIA, risultino rischi elevati per gli interessati, **spetta al titolare individuare le misure di sicurezza o altre modalità di diminuzione del rischio da adottare**

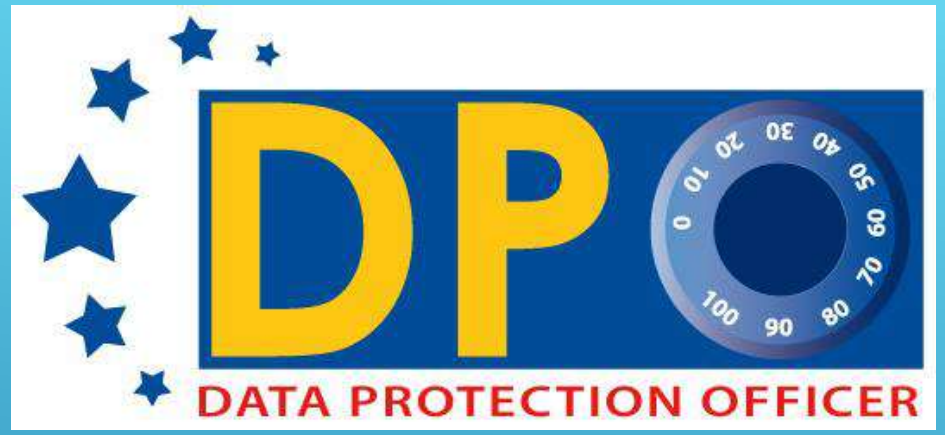
accountability

Le Linee guida affrontano anche il tema della **consultazione preventiva dell'Autorità garante**.

- **Il WP29 afferma che il ricorso alla consultazione dell'Autorità di controllo è necessario solo laddove il titolare non può/non riesce a mettere in atto misure sufficienti di attenuazione del rischio ad un livello accettabile.**

- **RISK ANALYSIS** = fase necessaria per ogni trattamento e prima questo abbia inizio (privacy by design)
- **VALUTAZIONE DEL RISCHIO** = processo costante
- **ACCOUNTABILITY** = attribuzione esclusiva alla responsabilità del titolare di ogni decisione sia sulla valutazione della elevatezza o meno dei rischi, sia dell'eventuale esistenza di rischi così elevati da rendere necessario il ricorso preventivo all'Autorità di controllo

RISK MANAGEMENT E DPIA



Il DPO (artt. 37- 38 - 39 del GDPR) svolge compiti di **informazione e consulenza** al titolare, al responsabile del trattamento e ai dipendenti circa i contenuti della normativa privacy, di **formazione** del personale addetto al trattamento dei dati, di **sorveglianza** nell'adempimento della disciplina relativa alla privacy. E' anche l'interlocutore dell'Autorità di controllo.
Viene nominato dal titolare o dal responsabile, agisce in piena **autonomia ed indipendenza** ed in **assenza di conflitti di interesse**.

La nomina del DPO è adempimento obbligatorio laddove il titolare:

- è **autorità/organismo pubblico** (eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali)
- effettua trattamenti che richiedono il **monitoraggio regolare e sistematico** degli interessati su **larga scala**
- effettua come attività principali **trattamenti su larga scala di dati sensibili, genetici, biometrici, giudiziari**.

IL DATA PROTECTION OFFICER

In caso di **violazione di dati personali**:

- il titolare «notifica la violazione all'autorità di controllo competente.. 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.. non sia effettuata entro 72 ore, è corredata dai motivi del ritardo» (art. 33 par. 1 del GDPR);

- il responsabile del trattamento «informa il titolare **senza ingiustificato ritardo** dopo essere venuto a conoscenza della violazione (art. 33 par. 2 del GDPR).

In relazione alla violazione del Regolamento UE (art. 83 del GDPR) sono previste **sanzioni amministrative pecuniarie**:

- **fino a € 10.000.000 e, per le imprese, fino al 2% del fatturato mondiale totale annuo** (es. mancata o errata comunicazione all'autorità competente di data breach, violazione dell'obbligo di nomina di DPO, mancata applicazione di misure di sicurezza)

- **fino a € 20.000.000 e, per le imprese, fino al 4% del fatturato mondiale totale annuo** (es. trasferimento illecito di dati personali ad un Paese terzo, inosservanza di una limitazione posta dall'autorità competente).

DATA BREACH – SANZIONI -

VIOLAZIONE GDPR: IL CASO CAMBRIDGE ANALYTICA

L'Information Commissioner's Office (Ico), cioè l'ente britannico per la protezione dei dati personali, ha inflitto una multa di 500 mila sterline, pari a 565 mila euro, a Facebook in relazione allo scandalo Cambridge Analytica. La società di Zuckerberg è stata accusata di **mancanza di trasparenza e di non essere riuscita a proteggere le informazioni degli utenti.** Il gigante dei social media ha difatti permesso alla app di Kogan di accedere ai dati dei suoi utenti senza riuscire ad impedire che venissero cedute a terzi, dimostrando di **non aver messo in atto adeguate misure di sicurezza.**

VIOLAZIONE GDPR: FACEBOOK E CAMBRIDGE ANALYTICA

UPCOMING CHALLENGES

Marketing telefonico e pubblicità

Cyberbullismo e fake news

La difesa dei minori

L'associazionismo politico

La minaccia cinese

Cybercrime

DIGITAL LIFE IN 2025

“There is no law of physics that says that it is impossible to have privacy. We can have privacy, if that is what we as a society choose.”

— BARBARA SIMONS, A HIGHLY DECORATED RETIRED IBM COMPUTER SCIENTIST, FORMER PRESIDENT OF THE ACM, AND CURRENT BOARD CHAIR FOR VERIFIED VOTING