monokee

Login once, run everywhere.

# IAM e GDPR:

## interconnessioni, implicazioni

## p o t e n z i a l i t à

# SOMMARIO

# INTRODUZIONE

A partire dal 25 maggio 2018, il **Regolamento generale sulla protezione dei dati** (GDPR) ha radicalmente cambiato il modo in cui le organizzazioni sono tenute a raccogliere, conservare e trattare i dati personali.
L'aspetto chiave è che qualsiasi informazione in grado di identificare una persona deve essere protetta in tutte le fasi della sua gestione, al fine di prevenire perdite di dati, violazioni (cosiddetti *data breaches*) e qualsiasi trattamento illecito di dati personali.
La nuova normativa capovolge quindi la prospettiva tra individui ed organizzazioni, andando a conferire agli utenti il pieno controllo su come le proprie informazioni vengano raccolte, gestite, trattate e condivise durante l'intero **ciclo di vita** del dato.

Al giorno d'oggi, la protezione delle informazioni si sgancia sempre più da una strategia basata sulla difesa del perimetro fisico aziendale, per avvicinarsi gradualmente ad una nuova linea di protezione basata sull'**identità digitale** e sulla **gestione degli accessi**. Pertanto, la domanda principale a cui le organizzazioni si trovano a dare risposta non è più "dove" siano fisicamente ubicate le informazioni bensì "**chi**" abbia accesso a tali risorse.
Appare interessante notare come il GDPR non faccia riferimento al "come" l'organizzazione sia tenuta, nel pratico, a soddisfare i requisiti imposti dall'articolo 5 all'articolo 32 relativi alla gestione degli accessi e alla sicurezza dei trattamenti, tanto da far emergere quello che viene definito da alcuni un "*technological gap*".

La risposta a questa lacuna è fornita in larga parte dalle piattaforme di **Identity and Access Management**. Un'efficace gestione IAM è infatti un'ottima soluzione per garantire che le informazioni (tra cui spiccano le identità digitali) siano accessibili solamente al personale autorizzato, rispettando gli stringenti requisiti di sicurezza richiesti dal GDPR.

# CAPITOLO 1

## IDENTITY and ACCESS MANAGEMENT COME RISPOSTA STRATEGICA AL GDPR

Considerando i principali ambiti di applicazione del GDPR, l'implementazione di una piattaforma IAM si rivela di strategica importanza in una molteplicità di aree:

### GESTIONE DATI PERSONALI

Principio cardine del GDPR è indubbiamente la protezione dei dati personali contro il trattamento illecito e/o non autorizzato.

Una piattaforma centralizzata di IAM, basata su specifiche *policies* di accesso e possibilmente rafforzata da meccanismi di autenticazione multifattore, **assicura che solamente gli utenti (o i ruoli) autorizzati possano accedere a determinate risorse**.
Un sistema IAM garantisce inoltre una **tracciabilità** importante in merito a chi ha effettuato il log-in, quando e a quali dati ha avuto accesso, permettendo di gestire rapidamente la concessione e la revoca degli accessi, attraverso meccanismi di autenticazione federata.

### SICUREZZA DEL TRATTAMENTO

Secondo l'articolo 32 GDPR il Titolare del trattamento e il Responsabile del trattamento sono tenuti a mettere in atto "*misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*".



In particolare, devono sussistere la "*capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento*" e "*la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico*".
Centrale è altresì l'obbligo di definire "*una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*". Ovviamente la sicurezza non vale solamente per i trattamenti nuovi, avvenuti dopo il 25 maggio 2018, bensì per tutti i trattamenti di dati personali in essere all'interno dell'organizzazione.

Conformemente con quanto richiesto dal GDPR, un'efficace piattaforma IAM **riduce il rischio associato alla perdita di dati e ad accessi non autorizzati**.
Allo stesso tempo, in caso di *data breach*, garantisce una **rapida identificazione dai dati personali sottoposti a violazione**.
Conformemente agli articoli 6, 25, 32 GDPR, è essenziale prevedere meccanismi di **pseudonimizzazione** degli eventi di audit e sistemi di **crittografia** dei dati, al fine di mettere in atto misure tecniche e organizzative che assicurino un livello di sicurezza appropriato al rischio.

## CONSENSO INFORMATO

Secondo l'articolo 4 GDPR, per **CONSENSO** si intende "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*."

Quando si richiede il consenso è necessario tenere presente che la volontà manifestata dall'utente deve essere:

- **LIBERA**: l'utente deve poter scegliere se accettare o rifiutare il trattamento dei suoi dati personali. Inoltre, deve essere concessa la possibilità di modificare facilmente la propria scelta in ogni momento;
- **SPECIFICA**: la manifestazione di volontà deve riferirsi al trattamento di un particolare dato o di una categoria limitata di dati;
- **INFORMATA**: l'utente deve disporre delle informazioni necessarie per formulare un proprio giudizio sull'opportunità di dare o meno il consenso. Tali informazioni devono essere disponibili prima di qualunque trattamento di dati personali;
- **INEQUIVOCABILE**: il consenso, per essere considerato tale, deve consistere in una dichiarazione di volontà o un atto chiaramente affermativo.

La soluzione ideale sarebbe quella di richiedere agli utenti un **consenso** cosiddetto **GRANULARE**, ossia richiedere un consenso per ciascun tipo di dati ai quali l'applicazione intende accedere. In questo modo gli interessati possono verificare con esattezza quali funzioni comportano un trattamento e quali dati saranno processati.
Un simile approccio soddisfa contemporaneamente due importanti requisiti giuridici: in primo luogo quello di informare adeguatamente l'utente in merito a elementi importanti del servizio offerto, e in secondo luogo quello di chiedere il consenso specifico per ognuno di essi.



Ovviamente, anche qualora il consenso soddisfi tutti gli elementi sopra descritti, questo non concede l'autorizzazione a trattamenti sleali o illeciti. Se il trattamento è eccessivo e/o sproporzionato rispetto alla finalità, anche se l'utente vi ha acconsentito, il titolare non disporrà di un fondamento giuridico valido, violando i requisiti del GDPR.

In ogni caso, ai sensi dell'articolo 7 del GDPR, qualora il trattamento sia basato sul consenso, il Titolare del trattamento deve essere in grado di **dimostrare** che l'interessato ha espresso il proprio consenso al trattamento dei dati personali. Inoltre, l'organizzazione deve essere preparata a gestire richieste di revoca/modifica dei dati da parte degli utenti, i quali possono anche inoltrare domanda per ottenere il **backup** dei propri dati in un formato interscambiabile.

**Il dato personale è quindi un'informazione che l'organizzazione deve essere in grado di recuperare in ogni momento.**

Attraverso un'efficace piattaforma IAM la gestione dei consensi può essere semplificata, in quanto la maggior parte dei consensi raccolti saranno **gestiti e registrati in modo centralizzato** attraverso i profili utente.
Sarà inoltre possibile disporre di una **lista dei consensi raccolti**, permettendo in itinere la possibilità di ritirare il consenso prestato da parte dell'utente, fino alla possibilità di fornire **report di audit** per monitorare i consensi dati e negati.

## MINIMIZZAZIONE DEI DATI

Un concetto sostanziale del GDPR è la cosiddetta "***data minimization***", connessa al divieto di trattare una quantità maggiore di dati rispetto a quella necessaria (minima) per svolgere i propri processi essenziali.

Attraverso una piattaforma IAM si ha un **controllo centralizzato degli accessi e delle autorizzazioni**, definendo i **periodi di tempo e la quantità di informazioni a cui garantire l'accesso**, gestendo altresì l'eliminazione delle informazioni legate agli account non più utilizzati.
Oltre a ciò, un sistema IAM adeguatamente integrato, è in grado di fornire informazioni in merito agli accessi alle applicazioni, conoscendo chi ha avuto accesso a quali dati.
Primaria deve essere l'attenzione posta al meccanismo di "***Access Recertification***" secondo cui l'organizzazione deve regolarmente ri-certificare gli accessi degli utenti per assicurare che ognuno possegga il corretto livello di autorizzazione, **monitorando ogni cambio di status** e rimuovendo tempestivamente i cosiddetti "*ghost accounts*".

## SEPARAZIONE DEI COMPITI E MINIMO PRIVILEGIO

In linea con il concetto di minimizzazione dei dati troviamo altri due principi a cui una piattaforma IAM permette di conformarsi. Il primo è il principio della separazione dei compiti (***Segregation of Duties***) che richiede l'azione da parte di più di un utente aziendale per portare a termine azioni riguardanti il trattamento di dati personali. Il concetto di minimo privilegio (**Least Privilege**) prevede invece che ad ogni utente sia garantito il minimo ammontare di accesso, conformemente con il proprio ruolo.

Se gli accessi devono essere tenuti al minimo, linea contraria va mantenuta per quanto riguarda i sistemi di **AUTENTICAZIONE**, la cui sicurezza va impostata sui maggiori livelli possibili.



In linea con questa prospettiva, per gestire in maniera centralizzata gli accessi alle molteplici applicazioni che l'azienda utilizza, è possibile ricorrere alla tecnologia ***Single Sign On***, con la quale unificare e strutturare le procedure di log in. Per rafforzare la sicurezza in un contesto *Single Sign On,* coniugando la facilità di accesso con la protezione dei dati, sono sempre più diffuse le tecniche di **Strong Authentication**, come per esempio l'autenticazione multifattore, che richiede l'utilizzo contemporaneo di più fattori per verificare l'identità dell'utente.

I concetti fin qui esposti possono essere racchiusi nei due elementi principali attorno ai quali si snoda il GDPR ossia le nozioni di:

**PRIVACY BY DESIGN**:

incorporare il rispetto della privacy fin dalla progettazione dei sistemi, attraverso *un risk-based approach*.

**ACCOUNTABILITY**:

responsabilizzazione e rendicontabilità

# CAPITOLO 2

## IDENTITY and ACCESS MANAGEMENT COME PROVA DI CONFORMITÀ

Secondo il concetto di **accountability** viene posta in capo al Titolare del trattamento la responsabilità di determinare il rischio di impatto che il trattamento può avere sui diritti e sulle libertà degli interessati e, al contempo, di dimostrare che la valutazione del rischio e la predisposizione di misure tecniche e organizzative provengano da scelte ponderate e documentabili.

Le cosiddette "***proofs of compliance***" rappresentano un elemento chiave nella prospettiva promossa dal GDPR.
Una piattaforma IAM in cui siano integrate funzioni di ***Analytics & Intelligence*** fornisce al Titolare del trattamento un ulteriore strumento di reportistica e tracciabilità delle attività inerenti la gestione delle identità e degli accessi, durante l'intero ciclo di vita delle utenze. Tale reportistica permette di evidenziare l'andamento degli accessi e dei diritti connessi (*entitlement*), garantendo la repentina identificazione di eventi sospetti nell'ottica del cosiddetto *risk-driven approach*.

In questo modo, una piattaforma IAM sarà in grado di fornire informazioni ulteriori rispetto a chi siano gli utenti e a cosa essi abbiano accesso, per fornire una più completa reportistica in merito a come siano utilizzati nel concreto i privilegi di accesso.



Molteplici sono i benefici di una piattaforma IAM integrata con funzioni di ***Analytics & Intelligence:***

### IDENTIFICARE I RISCHI IN MODO SEMPLICE E TEMPESTIVO (Risk Analysis)

Attraverso la tracciabilità degli eventi è possibile monitorare le attività considerate più esposte ai rischi, siano queste esercitate da un amministratore o da un utente, come violazioni del principio di *Segregation of Duties*, cambi password, assegnazioni dirette, autenticazioni fallite…

### TRACCIARE GLI EVENTI ED ANALIZZARNE I TREND (Audit Event Analysis)

Gli strumenti di *Analytics & Intelligence* permettono un auditing approfondito della piattaforma IAM attraverso l'analisi di diverse fonti di dati a diversi livelli di approfondimento, rappresentando il tutto in semplici dashboard personalizzabili ed esportabili. Partendo dall'identificazione dei cosiddetti *Key Risk Indicators (KRIs)* del proprio business è possibile tracciarne l'andamento nel tempo, monitorando eventuali comportamenti anomali (ad esempio richieste ripetute di diritti eccezionali da parte di un utente).

### SORVEGLIARE LE CONDOTTE SOSPETTE

La possibilità di tenere traccia degli eventi che accadono sulla propria piattaforma IAM permette di indagare le cause di eventuali condotte anomale o che non coincidono con un utilizzo regolare della piattaforma. In questo modo, dopo aver individuato l'origine dell'anomalia, è possibile adottare misure di sicurezza preventive per scongiurare che gli eventi sospetti si traducano in danni reali per l'organizzazione (per esempio agendo sulle *policies* di accesso).

## MIGLIORARE E VELOCIZZARE I PROCESSI DECISIONALI

Avere a disposizione analisi, statistiche e trend costantemente aggiornati permette di ottimizzare i processi decisionali.
Le funzioni di *Analytics & Intelligence* rispondono infatti ad una prospettiva *business-oriented* in grado di condurre i decisori verso un miglioramento dei processi di governance e di amministrazione.
A ciò si somma la possibilità di filtrare gli eventi secondo diversi criteri (esempio per data, categoria, tipologia…), al fine di rendere più veloce e completa la presa di decisioni.

## OTTIMIZZARE I COSTI

La possibilità di analizzare i trend di accesso e di utilizzo delle applicazioni collegate alla piattaforma di IAM, permette di verificare se i costi sostenuti dall'organizzazione per il possesso delle varie applicazioni sia in linea con i dati di utilizzo delle stesse.

Un'implementazione di questo tipo consente di mitigare una delle principali preoccupazioni che, al giorno d'oggi, coinvolge i vertici aziendali in materia di sicurezza, ossia la scarsa visibilità delle minacce a cui l'organizzazione è esposta, non disponendo di una reportistica completa e costantemente aggiornata.

Oltre a ciò, per aziende di grandi dimensioni, diviene sempre più complicata la gestione di migliaia di utenti, ognuno con il proprio ruolo e i propri diritti di accesso da tenere sotto controllo. Tutto ciò incrementa considerevolmente i rischi per la sicurezza, così come inefficienze organizzative, perdite di dati e mancata compliance con le normative.



L'integrazione di una piattaforma IAM con funzionalità di *Analytics & Intelligence* permette all'organizzazione di ottenere un duplice vantaggio in termini di Security e Compliance.

La documentazione estraibile da una piattaforma così integrata è infatti in linea con il principio di ***accountability*** portato avanti dal GDPR, consentendo al Titolare del trattamento di disporre della documentazione volta ad attestare di aver intrapreso fin dal principio le misure adeguate a mitigare il rischio di *data breach*.

Tuttavia, è sempre necessario tenere presente che il concetto di *Accountability* deve viaggiare di pari passo con il concetto di ***Privacy by Design***. Il rispetto della normativa di Data protection deve infatti essere garantito anche nell'implementazione delle funzionalità di *Analytics and Intelligence*, che non possono prevedere un trattamento di dati in maniera non conforme al GDPR.
È quindi necessario compiere ragionamenti preventivi su molteplici fronti: dall'raccolta dei **consensi** (successiva alla predisposizione di un'informativa), alle procedure di **pseudonimizzazione** dei dati, fino alle modalità di **conservazione** degli stessi, il tutto all'interno di un "Documento di Politica di utilizzo dei dati".

# CAPITOLO 3

## ULTERIORI ELEMENTI GIURIDICI DA CONSIDERARE PER ESSERE GDPR COMPLIANT

### LEGGE APPLICABILE (articolo 3)

In base all'articolo 3 GDPR, la normativa comunitaria "*si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*".

Inoltre "*il Regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione effettuato da un titolare del trattamento o responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:*
*a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato, oppure*
*b) il controllo del loro comportamento, quest'ultimo inteso all'interno dell'Unione europea.*"

Infine *"il Regolamento si applica anche al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto nazionale di uno Stato membro in virtù del diritto internazionale pubblico.*"



### LICEITÀ DEL TRATTAMENTO E DEFINIZIONE DEI RUOLI (articoli 4 e 6)

Una necessità primaria è quella di identificare i **ruoli** dei soggetti coinvolti, definendo fin dal principio chi riveste il ruolo di Titolare del trattamento e di Responsabile del trattamento.
La definizione dei ruoli, supportata da un'adeguata documentazione, consentirà quindi di individuare le **responsabilità** in caso di trattamento illecito di dati.

**Titolare del trattamento**: è la "*persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, **determina** la **finalità** e i **mezzi** del trattamento di dati personali*".

**Responsabile del trattamento**: è la "*persona fisica, giuridica, pubblica amministrazione o ente che **elabora i dati personali per conto del titolare** del trattamento*".

### DATA PROTECTION IMPACT ASSESSMENT (articolo 35)

Secondo l'articolo 35 GDPR, *"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. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi"*

La Valutazione di impatto (DPIA) quindi, oltre ad essere un ulteriore obbligo sancito dal GDPR, rappresenta anche uno strumento importante in termini di responsabilizzazione (***accountability***) in quanto aiuta il Titolare del trattamento non soltanto a rispettare i requisiti GDPR, ma anche ad attestare di aver implementato misure idonee a garantire il rispetto del regolamento.

La Valutazione di impatto ricade sotto la responsabilità del Titolare del trattamento e deve essere prevista prima di procedere al trattamento dati e conseguentemente sottoposta ad un riesame continuo.

## DATA PROTECTION OFFICER (articoli 37, 38, 39)

Una figura introdotta dal GDPR è il *Data Protection Officer* (comunemente chiamato DPO o, in italiano, Responsabile della protezione dei dati).

Secondo la normativa europea, devono designare obbligatoriamente un DPO:
a) amministrazioni, enti pubblici e autorità giudiziarie nell'esercizio delle loro funzioni;
b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
c) tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Nominato dal Titolare del trattamento, con conseguente comunicazione al Garante, il DPO è un **consulente esperto** che affianca il Titolare nella gestione delle problematiche relative del trattamento dei dati personali. Questa figura si occupa in maniera esclusiva della materia della protezione dei dati personali, aggiornandosi sui rischi e sulle misure di sicurezza.



Conformemente al principio di *accountability* su cui si fonda il GDPR, la figura del DPO facilita Titolare e Responsabile nel rispetto dei requisiti richiesti dal Regolamento.

Nello specifico, il DPO si occupa di:

a) sorvegliare l'osservanza del regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
b) collaborare con il Titolare/Responsabile, laddove necessario, nel condurre la Valutazione di impatto sulla protezione dei dati (DPIA);
c) informare e sensibilizzare il Titolare o il Responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal GDPR e da altre disposizioni in materia di protezione dei dati;
d) cooperare con il Garante e fungere da punto di contatto tra l'organizzazione e il Garante su ogni questione connessa al trattamento;
e) supportare il Titolare o il Responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un Registro delle attività di trattamento.

Aspetto centrale di questa figura è la sua **indipendenza** ed **autonomia** rispetto all'azienda: egli infatti tutela i dati personali, non gli interessi del Titolare del trattamento. Egli deve agire in totale assenza di conflitto di interessi, quindi non deve essere nelle condizioni di poter influenzare scelte in merito al trattamento di dati personali, né ricevere istruzioni su come eseguire i propri compiti.
Per questo motivo, solitamente le organizzazioni decidono di ricorrere a un DPO esterno, poiché è difficile pensare ad una condizione di autonomia all'interno di un rapporto di lavoro dipendente.

## REGISTRO DEI TRATTAMENTI (articolo 30)

Parte integrante di un sistema di corretta gestione dei dati personali è la tenuta del cosiddetto Registro dei Trattamenti. Secondo l'articolo 30 del GDPR tale Registro va tenuto **in forma scritta, in formato elettronico, e deve essere esibito su richiesta al Garante.**

L'articolo in questione elenca una lista di contenuti minimi che devono essere obbligatoriamente presenti nel Registro dei Trattamenti:
*- il **nome e i dati di contatto** del Titolare del trattamento, del Rappresentante e dell'eventuale Responsabile della protezione dei dati (DPO);*
*- le **finalità** del trattamento;*
*- una **descrizione** delle categorie di interessati e delle categorie di dati personali trattati;*
*- le categorie di **destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;*
*- ove applicabile, **i trasferimenti di dati personali verso un paese terzo** o un'organizzazione internazionale;*
*- ove possibile, i **termini ultimi previsti per la cancellazione** delle diverse categorie di dati;*
*-ove possibile, una **descrizione** generale delle **misure di sicurezza tecniche e organizzative** adottate.*

**L'obbligo di redazione e adozione del Registro non è generale**: infatti il paragrafo 5 dell'articolo 30 specifica che esso non compete *"alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10."*

Al di là di essere un obbligo normativo, la tenuta di un Registro dei trattamenti rappresenta un importante strumento per aumentare la **consapevolezza** dei processi che avvengono all'interno dell'organizzazione.



In questo modo, oltre a fungere da "***proof of compliance***" per il GDPR, tale Registro permette di conoscere nel dettaglio i meccanismi sottostanti il trattamento dei dati.

## DIRITTO ALL'OBLIO (articolo 17)

Secondo l'articolo 17 GDPR, **"***l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali.*

L'incremento dei diritti degli utenti nella gestione dei propri dati comprende anche il cosiddetto Diritto all'oblio (*Right to be Forgotten),* ossia il **diritto di ottenere la cancellazione (o la rettifica) dei propri dati, a cui il Titolare deve provvedere senza ingiustificato ritardo**.
In particolare, l'interessato ha il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti, qualora abbia ritirato il consenso, si sia opposto al trattamento o qualora il trattamento dei suoi dati personali non sia conforme al Regolamento.
Si badi che i dati cancellati non possono essere in nessun caso sottoposti a backup o essere resi nuovamente accessibili.
Per rafforzare il "diritto all'oblio" nell'ambiente on line, è opportuno che il diritto di cancellazione sia esteso in modo da **obbligare il Titolare del trattamento ad informare i Responsabili del trattamento affinché cancellino qualsiasi link verso tali dati personali, copia o riproduzione di detti dati**.
L'articolo 17 precisa, comunque, che il Diritto all'oblio non è assoluto, ma presenta alcune limitazioni. In particolare, la libertà di espressione, il pubblico interesse, ed anche interessi storici, statistici e di ricerca scientifica, possono consentire il mantenimento dei dati personali nonostante l'opposizione dell'interessato.

## NOTIFICA DI DATA BREACH
## (articoli 33 e 34)

All'articolo 33 il GDPR prevede che, in caso di violazione di dati personali, il Titolare del trattamento è obbligato a notificare tale evento al Garante senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne sia venuto a conoscenza**.

Con il provvedimento n. 157 del 30 luglio 2019, il Garante ha introdotto un **nuovo modulo di notifica**, richiedendo al Titolare di raccogliere una lunga serie di informazioni relative alla violazione, aumentando quindi l'onerosità di tale notifica.
Nello specifico, oltre ai dati del soggetto che effettua la notifica e quelli del Titolare del trattamento, è necessario fornire informazioni dettagliate relativamente alla violazione, alla sua gravità e alle possibili conseguenze. Va altresì specificato quali contromisure sono state applicate per limitare l'impatto della violazione e come si intende agire per prevenire un eventuale ripresentarsi del problema.
In un'altra sezione occorre specificare se la violazione sia stata comunicata o meno agli interessati.

A questo proposito, l'articolo 34 del GDPR sancisce che qualora la violazione sia "*suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo*".

Sono però previste tre eccezioni a tale obbligo di comunicazione:
1. Il titolare del trattamento aveva implementato misure tecniche e organizzative adeguate anche ai dati personali oggetto di violazione (primaria, in questo caso, la **cifratura**);
2. Il titolare del trattamento ha successivamente adottato misure volte a scongiurare il sopraggiungere di rischi per i diritti e le libertà dell'interessato;
3. La comunicazione richiederebbe sforzi sproporzionati (viene sostituita, in questo caso, da una comunicazione pubblica).



L'aumento degli oneri connessi alla notifica di *data breach* va visto quindi in una duplice accezione: da una parte, permette al Titolare di assumere piena conoscenza della portata della violazione avvenuta, dall'altra, permette di valutare in maniera accorta se vi sia la necessità di comunicare o meno l'accaduto alle persone fisiche interessate.

Il procedimento di notifica deve essere supportato dalla tenuta, da parte del Titolare del trattamento, del cosiddetto "**Registro delle violazioni**": un documento che ha la duplice funzione di consentire al Titolare il monitoraggio di tutte le violazioni di dati personali avvenute nel corso delle proprie attività di trattamento, e al Garante di verificare il rispetto dell'obbligo di notifica tempestiva.

Sanzioni fino a

**€ 20 milioni**

oppure il

**4 % del volume d'affari**

globale annuo dell'azienda

# CAPITOLO 4

## REQUISITI GDPR PER L'IMPLEMENTAZIONE DI UN NUOVO PROGETTO IT

Dall'entrata in vigore del GDPR, conformemente ai principi di *privacy by design* e *privacy by default*, diviene necessario tenere presente il rispetto della privacy fin dalle prime fasi di implementazione dei nuovi progetti, in particolare se questi prevedono un trattamento automatizzato di dati personali.

Nello specifico, vanno soddisfatti i seguenti requisiti:

- REQUISITI FUNZIONALI ESPLICITI: rappresentano le esigenze funzionali che il servizio IT deve soddisfare per generare valore per chi lo utilizza;
- REQUISITI FUNZIONALI IMPLICITI: rappresentano esigenze funzionali sottese al servizio che si sta offrendo, come le regole di profilazione degli utenti che accedono ad un sistema e i diritti di accesso alle varie categorie di dati per i singoli profili degli utenti;
- REQUISITI NON-FUNZIONALI: comprendono le caratteristiche organizzative e tecniche che il servizio IT dovrà rispettare;
- REQUISITI DI QUALITÀ E DI SICUREZZA: riferendosi al modello ITIL, comprendono ciò che funge da "garanzia" per il servizio offerto, rappresentandone la qualità. Tra i requisiti più importanti emergono la disponibilità, la capacità, l'affidabilità e la sicurezza del servizio.

Si noti che tali requisiti, inerenti gli standard di *Business Analysis*, rispecchiano perfettamente quanto richiesto dal GDPR, evidenziando quindi la complementarietà tra il Regolamento europeo ed i modelli di organizzazione aziendale.



Traducendo quindi i requisiti di Business in requisiti di Data protection, emergono le seguenti qualità da rispettare durante il trattamento dei dati:

- DISPONIBILITÀ: il dato deve essere fruibile per gli utenti attraverso il servizio IT che lo tratta;
- RISERVATEZZA: il dato deve essere accessibile soltanto da parte di chi riveste un ruolo che ne consente l'accesso;
- INTEGRITÀ: il dato deve essere protetto rispetto ad inappropriate modifiche di contenuto, siano esse accidentali oppure non autorizzate;
- ESATTEZZA: i dati personali devono essere corretti, sempre aggiornati, eliminati o modificati quando inaccurati;
- CONFORMITÀ: il dato deve essere espresso conformemente alle leggi e ai regolamenti vigenti.

A ciò si sommano due ragionamenti da fare in merito alla salvaguardia dei dati:

- RTO (*Recovery Time Objective*): tempo totale necessario per il ripristino della piena funzionalità di un servizio IT, comprensivo dei dati in esso contenuti, in caso di incidente;
- RPO (*Recovery Point Objective*): tempo nel passato cui è possibile tornare con il ripristino dei dati. In altre parole, questo concetto può essere espresso come il massimo ammontare di dati che l'organizzazione è disposta a perdere in caso di incidente.

**Tutti i requisiti fin qui elencati, letti nell'ottica della GDPR compliance, vanno affrontati in modo sistematico fin dall'inizio ed implementati fin dalla progettazione dei servizi IT, in altre parole *by design*.**

## FASI DA SEGUIRE PER IMPLEMENTARE UN PROGETTO GDPR COMPLIANT:

1. ANALISI DEL RISCHIO:

- individuare tutti i rischi (eventi casuali e non) che possono alterare il risultato atteso, basandosi sull'esperienza, *good practices* ed altre metodologie codificate;
- quantificare la probabilità di accadimento di tali eventi;
- quantificare il peso del rischio rinvenuto (moltiplicando l'impatto per la probabilità di accadimento);
- costruire una scala dei rischi, da quelli più pesanti a quelli più leggeri;
- stabilire quali azioni possono mitigare probabilità e/o impatto dei rischi analizzati, insieme al loro costo;
- rivalutare il rischio alla luce delle contromisure considerate.

2. CIRCOSCRIZIONE DEL PERIMETRO DEL TRATTAMENTO: quali dati saranno trattati? qual è lo scopo del trattamento? Per quanto tempo saranno conservati? Se si parla di dati personali, questi saranno assoggettati a tutte le regole del GDPR;

3. REDAZIONE DEL DOCUMENTO DI POLITICA DI UTILIZZO DEI DATI: attraverso le opportune analisi, questo documento dovrà contenere informazioni relative ai dati che vengono raccolti, lo scopo e le modalità di utilizzo dei dati, il tempo di conservazione ed il metodo di protezione implementato.

4. RACCOLTA DEI DATI E CONSENSO: la raccolta dei dati deve avvenire al momento della stipula del contratto, insieme al consenso informato (firmato dal cliente) con tutte le specificazioni richieste dal GDPR;

5. CORRETTA ARCHIVIAZIONE DEI CONTRATTI E DEI CONSENSI: applicare misure adeguate volte ad impedire accessi non autorizzati ai dati personali, consentendo l'inserimento dei dati personali solamente al personale autorizzato.

6. APPLICAZIONE DI TUTTI I REQUISITI DI SICUREZZA AI DATI: coniugare le richieste del GDPR con i requisiti funzionali, non funzionali e di qualità della Business Analysis, verso una sicurezza globale ed integrata.
   A ciò si somma la previsione di eventuali sistemi di Firewall, crittografia, pseudonimizzazione, regole di accesso, backup e ripristino, gestione password, controllo qualità…

7. BILANCIAMENTO E RICALIBRAZIONE CONTINUI: la normativa GDPR prevede che queste analisi siano ripetute periodicamente, al fine di mantenere sempre aggiornata la valutazione dei rischi e la protezione dei dati personali.

# CONCLUSIONE

Alla luce dell'analisi fin qui presentata, appare evidente come l'adeguamento alla normativa privacy possa rappresentare una **strategia** volta ad accrescere la conoscenza della propria organizzazione e quindi il proprio **vantaggio competitivo**, al di là di un mero recepimento di dettami legislativi per evitare di essere sanzionati.

Inoltre, i requisiti introdotti dal GDPR, essendo altamente **multidisciplinari**, sono pienamente in linea con le *good practices* e i principali standard internazionali come ITIL e COBIT, e gli standard relativi ai sistemi di gestione della sicurezza delle informazioni (ISO 27001), gestione del rischio (ISO 31000), business continuity (ISO 22301) e, più in generale, relativi alla qualità (ISO 9001).

Essere GDPR compliant è quindi un primo tassello, indispensabile e determinante, in grado di dirigere l'organizzazione verso una maggior **conoscenza** e **consapevolezza** dei processi interni, dei rischi, dei ruoli e dei flussi di dati, andando ad accrescere in ultima analisi la sicurezza aziendale.

**Poter contare su una solida piattaforma di Identity and Access Management, a sua volta rispondente ai requisiti di Data protection, rappresenta indubbiamente una risposta vincente al GDPR, garanzia di conformità e fonte di vantaggio competitivo.**

Adottando una prospettiva *risk-driven*, agevolata dall'integrazione di funzionalità di *Analytics & Intelligence* all'interno di una piattaforma IAM, è possibile passare da un atteggiamento consequenziale e repressivo ad una **visione proattiva e preventiva nella gestione della sicurezza aziendale**, pienamente in linea con l'approccio promosso dal GDPR.

monokee

Login once, run everywhere.

# CONTATTACI



Via Zeni Fortunato, 8, Rovereto, TN


+39 049 2970297


monokee@monokee.it

monokee.com