Pianificare, implementare, mantenere e migliorare un sistema di gestione privacy = Accountability

Flavia Montanile (*)

Il termine accountability è entrato prepotentemente a far parte della dialettica privacy a partire dall'ingresso del GDPR (General Data Protection Regulation), regolamento attraverso cui l'Unione Europea ha deciso di determinare i limiti entro cui muoversi per permettere una corretta e libera circolazione dei dati personali. Precedentemente sono stati emanati diversi decreti legislativi con lo stesso obiettivo, ma la responsabilizzazione del titolare del trattamento dei dati ha assunto un ruolo centrale dal 2016. Considerata la difficoltà riscontrata nella traduzione letterale, tale termine ad oggi viene utilizzato con l'intento di definire la responsabilizzazione del titolare, ovvero la sua accountability e dunque, la capacità di dimostrare la propria responsabilità per rendicontazione.

L'accountability del titolare è il filo conduttore che ci guida alla comprensione del GDPR e alle richieste che devono essere soddisfatte quando si decide di effettuare un trattamento, sia in qualità di titolare, sia di responsabile. Ma come si fa a stabilire se si è realmente un titolare che opera nel rispetto dell'accountability? È fondamentale conoscere e comprendere i principi espressi all'interno del Regolamento e utilizzare un approccio risk based oriented che punti al miglioramento continuo. Il focus di ciascuna valutazione/analisi effettuata preventivamente deve essere l'interessato e la tutela delle sue libertà fondamentali, applicando così il principio di Privacy By Design e Privacy By Default.

(*) Consulente gestione processi presso HQ Target **https://hqtarget.it/**

Il Sistema di Gestione Privacy

All'atto pratico, l'applicazione del principio dell'accountability consiste nel pianificare, implementare, mantenere e migliorare continuamente un sistema di gestione per la privacy.

Impostare la propria governance come un Sistema di Gestione facilita il compito di un titolare che intende effettuare i trattamenti in modo adeguato. Si può iniziare seguendo la struttura di una normativa ISO (High Level Structure – HLS) che comprende i seguenti punti:

- Campo di applicazione e contesto;
- Politica;
- Pianificazione;
- Risorse;
- Attività operative;
- Monitoraggio e misurazione;
- Miglioramento continuo.

Accountability

"The fact of being responsible for what you do and able to give a satisfactory reason for it […]. A situation in which someone is responsible for things that happen and can give a satisfactory reason for them"

Cambridge Dictionary

Campo di applicazione e contesto

Il titolare, prima di mettere in atto qualsiasi trattamento, deve analizzare il contesto nel quale opera.

Per contesto si può considerare sia la tipologia di dati che si andranno a trattare, sia la tipologia di interessati coinvolti nei trattamenti di futura implementazione. Per quanto concerne la tipologia di dati, infatti, il GDPR vieta di trattare i dati appartenenti a particolari categorie (art. 9), ovvero i dati cosiddetti sensibili: dati che rilevano lo stato di salute, dati rivelanti l'origine razziale o etnica, dati rivelanti l'appartenenza sindacale, dati che rivelano l'opinione politica, dati rivelanti l'orientamento sessuale, ecc. Queste tipologie di dati sono suscettibili di particolare attenzione per la loro delicatezza e per l'immane impatto che la loro divulgazione può arrecare all'interessato e necessitano quindi di particolari misure di sicurezza. Allo stesso modo, determinate categorie di interessati (come i dipendenti, gli anziani, i minori e i pazienti) necessitano di particolare riguardo poiché nel rapporto titolare-interessato ricoprono un ruolo più delicato, essendo la parte debole a livello contrattuale. Per *campo di applicazione* si può considerare quanto descritto al paragrafo 3 dell'articolo 35 del GDPR. Infatti, i casi in cui è richiesta la valutazione di impatto privacy (DPIA) fanno riferimento alle situazioni con rischio di impatto maggiormente elevato per i diritti e le libertà delle persone fisiche; un titolare si può ritenere accountable quando valuta il campo di applicazione e considera l'eventuale danno derivante dall'estensione del trattamento in anticipo rispetto all'attuazione del trattamento. Il campo di applicazione può quindi essere valutato considerando se si effettueranno la profilazione, il trattamento su larga scala o la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Politica

Uno degli impegni del titolare è quello di redigere una politica che abbia particolare riguardo alla privacy. Oltre a rientrare tra le misure di sicurezza a livello organizzativo e a rispettare i requisiti della normativa ISO/IEC 27701:2019 (Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines), la redazione della politica per la privacy è un passo fondamentale se si vuole raggiungere l'accountability.

In primo luogo, infatti, il GDPR richiede la responsabilità per rendicontazione e dunque la capacità di dimostrare la propria responsabilità. Successivamente bisogna considerare che la politica di un'azienda è il principale mezzo che l'Alta Direzione ha per comunicare alle parti interessate il core business aziendale. Infine, inserire nella propria mission l'impegno dell'alta direzione alla tutela dei dati personali fa comprendere anche ai "non addetti ai lavori" il ruolo centrale dell'interessato e della privacy a livello aziendale. La politica aziendale è infatti il primo messaggio che l'Alta Direzione invia ai propri collaboratori e con la quale dichiara la linea guida che intende seguire e far seguire. Dedicare una sezione alla tutela dei dati personali è un aspetto che rientra nell'essere rispettoso del principio di accountability.

Pianificazione

La pianificazione è la fase indispensabile per una corretta implementazione dei trattamenti e delle relative misure di sicurezza. Per *pianificazione* possiamo far riferimento all'articolo 25 del GDPR (Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita):"

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del 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, 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 tutelare i diritti degli interessati.
2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.[1] […]"

Perfettamente esplicitato all'interno dell'articolo, il titolare deve programmare fin dalla progettazione i mezzi e le misure di sicurezza adeguate a ciascun trattamento, tenuto conto del contesto e del campo di applicazione in cui opera. All'atto pratico, la progettazione fin dal principio consiste nell'utilizzare un approccio risk based, che consente al titolare di avere chiaro quali possono essere i rischi derivanti dall'attuazione di un determinato trattamento e successivamente quali contromisure o misure di sicurezza mettere in atto. Tale approccio consente al titolare di effettuare un'analisi delle minacce e di poter avere una panoramica di quelle che possono essere le carenze nel proprio Sistema di Gestione per la Privacy. In seguito all'effettuazione di un assessment e di una Gap Analysis, il titolare avrà piena contezza di quali possano essere le misure di sicurezza per i propri trattamenti. Questi elementi faranno parte della documentazione indispensabile per dimostrare la propria accountability. Di altrettanta rilevanza è l'articolo 35 del GDPR, ovvero quello descrivente la valutazione di impatto sulla protezione dei dati. Secondo il Regolamento, esistono particolari situazioni in cui è necessario effet-

[1] Art. 25 del Regolamento per la Protezione dei Dati Personali.

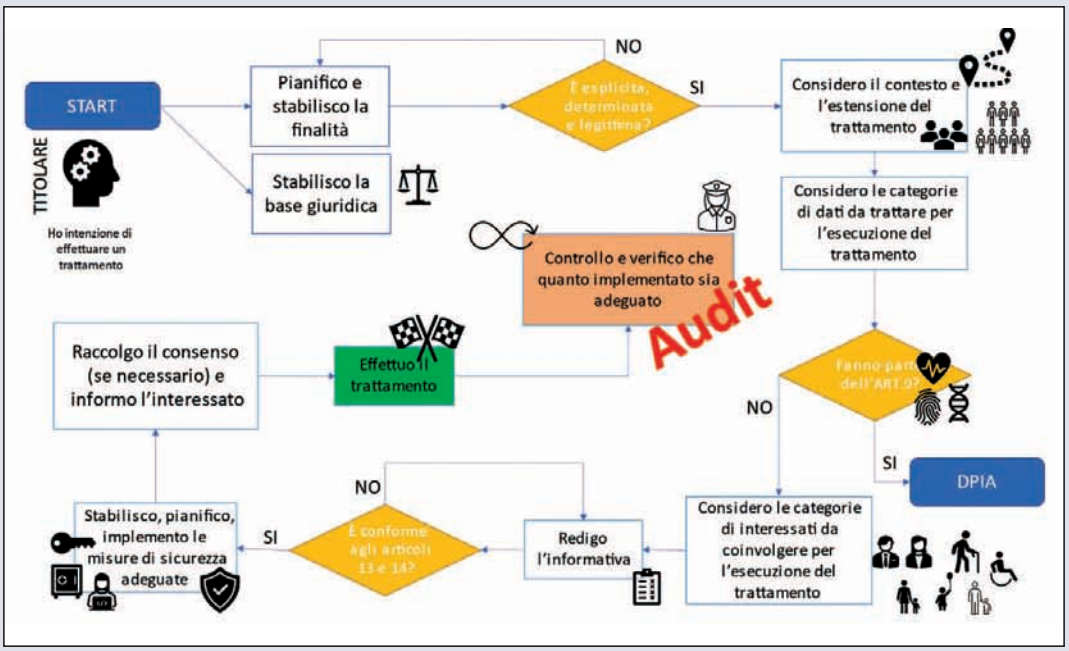

Figura 1- Pianificazione di un trattamento



tuare una valutazione preventiva di impatto privacy, ossia quando un trattamento – considerati la natura, l'oggetto, il contesto e le finalità del trattamento – comporta un rischio elevato per i diritti e le libertà delle persone fisiche. Fondamentalmente è bene applicare questo concetto in maniera preventiva per tutti i trattamenti che il titolare intende attuare, al fine di poter agire sempre in ottica privacy. Per questo processo il GDPR richiede informazioni documentate atte a testimoniare l'avvenuta valutazione, come descritto al par. 7 dell'articolo:

a. una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b. una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c. una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
d. le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Un titolare, che mantiene informazioni documentate aggiornate e coerenti con le fasi precedentemente descritte, avrà maggior facilità nell'applicare quanto descritto dall'art.35, trovando già punti di riferimento per la propria valutazione di impatto come il contesto, la finalità, gli asset utilizzati e tutti gli altri elementi considerati rilevanti per l'attuazione dei trattamenti nel ruolo di titolare.

Ovviamente, per poter dimostrare quanto pianificato, è bene conservare documenti che attestino l'analisi preventiva effettuata per ciascun trattamento, a prescindere dalla necessità di applicare quanto previsto dall'art.35.

Risorse

Un tassello fondamentale per la corretta implementazione dei propri trattamenti è la messa a disposizione delle risorse. Per il titolare sarà indispensabile aver cura di predisporre, oltre alle risorse strumentarie, economiche, finanziarie, tecniche e tecnologiche, anche quelle umane – l'aspetto più difficile da gestire. In ambito di accountability, rendicontare la propria efficienza è facile: politica comunicata alle parti interessate, privacy policy, procedura per la gestione delle password, pillole privacy pubblicate sulla intranet aziendale, informative infilate furtivamente tra le pagine dei contratti, badge e controllo accessi, avvertimenti su phishing e virus, e chi più ne ha più ne metta! Ciò che realmente risulta arduo da gestire è la propria efficacia: coinvolgere attivamente le risorse coinvolte nei trattamenti, renderle consapevoli, responsabilizzarle e sensibilizzarle; tutti obiettivi raggiungibili solo attraverso formazione ed informazione, coinvolgimento e motivazione. Aspetti di una delicatezza tale che non è possibile demandare. Ritorna centrale il ruolo della pianificazione e della consapevolezza del proprio campo di applicazione e contesto nel quale si opera in qualità di titolare: in base all'analisi effettuata precedentemente, ciascun titolare sarà in grado di riconoscere l'importanza e la centralità del ruolo delle proprie risorse e affiderà, in base al ruolo e alle caratteristiche di ciascuna di esse, il giusto compito con l'appropriata responsabilità.

Strumenti

Quali sono gli strumenti a disposizione del titolare? Anzitutto, la scelta del DPO (Data Protection Officer). Sarà colui che coordinerà ed orchestrerà il Sistema implementato insieme al titolare, sempre presente in anticipo e incessantemente pronto ad intervenire; indispensabile nelle organizzazioni con più di 250 dipendenti e per tutte quelle che effettuano trattamenti con dati particolari (art.9), consigliato in generale averlo nel proprio team. La scelta della persona che ricoprirà il ruolo del DPO è fortemente dibattuta oggi a causa dell'imparzialità che questi è tenuto ad avere nei confronti dell'organizzazione per la quale opera. È infatti sconsigliato selezionare tra i propri dipendenti, a meno che non si metta a disposizione del responsabile per la protezione dei dati un team che lo coadiuvi nelle scelte. Gli altri ruoli da attribuire, internamente all'organizzazione, sono gli autorizzati e gli Amministratori di Sistema (AdS). I primi possono essere suddivisi in due categorie: gli autorizzati e gli autorizzati con compiti speciali (o con compiti di coordinamento). I secondi, svolgendo attività di sovrintendenza alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione, devono rispondere a determinate caratteristiche per poter ricevere la nomina e svolgere, nel rispetto della tutela dei dati personali, la propria mansione. L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza[2]. Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante, al fine di rendicontare la propria responsabilità in qualità di titolare. L'assegnazione dei diversi incarichi avviene mediante documenti (nomine o autorizzazioni), che devono essere firmati e conservati per quanto appropriato. In detta documentazione dovrà essere chiaramente esplicitato il limite di azione di ciascuna risorsa, al fine di agevolare l'autorizzato e l'AdS nella comprensione delle proprie mansioni e delle proprie responsabilità. Altri incarichi che il titolare può affidare ed individuare sono i responsabili: persone fisiche o giuridiche che svolgono attività di trattamento per conto del titolare. Sono solitamente fornitori di servizi che collaborano con il titolare nello svolgimento di attività quali ad esempio la manutenzione dei sistemi operativi, le operazioni di backup, il servizio di guardiania, ecc. Con queste categorie, inoltre, deve esser firmato tra le parti un DPA (Data Processing Agreement), ovvero un contratto che delinea le responsabilità di ciascuna delle parti e tutela, nel caso di data breach, il responsabile che abbia rispettato le indicazioni descritte nell'accordo.

Attività operative

Con attività operative si può intendere la necessità di implementare le misure di sicurezza adeguate. Quando il GDPR utilizza l'aggettivo adeguato, intende sostanzialmente lasciare libertà di azione e massima responsabilità al titolare che, in seguito alle valutazioni effettuate preventivamente, sarà in grado di fronteggiare le minacce nella maniera più corretta. Le misure di sicurezza si suddividono in misure di sicurezza logiche/funzionali, fisiche ed organizzative. Le misure di sicurezza adeguate (e non più minime) richiedono al titolare un costante aggiornamento in merito ai requisiti cogenti, contrattuali, normativi e tecnologici. Ciò significa che a seconda del contesto, al variare dell'innovazione tecnologica o in seguito ad aggiornamenti/modifiche in ambito legale, il titolare dovrà nuovamente effettuare una valutazione della propria situazione (lo stato dell'arte) e considerare

[2] Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati... - Garante Privacy.

se quanto implementato sia ancora sufficiente a ricoprire i requisiti di sicurezza.
A supporto del titolare interviene la normativa UNI EN ISO/IEC 27001:2017 con la sua estensione ISO/IEC 27701:2019 che, attraverso la loro struttura, propongono una serie di controlli che è possibile implementare per poter migliorare in modo continuo il proprio Sistema di Gestione. La prima, è una normativa che permette l'implementazione del Sistema di Gestione per la Sicurezza delle Informazioni con l'obiettivo di rispettare la Riservatezza, l'Integrità e la Disponibilità delle informazioni. La seconda, in qualità di estensione della precedente, allarga i controlli applicabili alla sicurezza delle informazioni al contesto privacy. Un elemento che altresì può essere compreso nelle attività operative è la creazione del registro dei trattamenti, strumento principe del titolare che opera nel rispetto del principio dell'accountability. In esso, infatti, sono conservate (e mantenute aggiornate) tutte le informazioni inerenti i trattamenti in atto. Le informazioni registrate contengono gli attori coinvolti nel trattamento, gli asset utilizzati, il flusso dei dati (eventuali trasferimenti, destinatari), le categorie di interessati, le categorie di dati trattati e le misure di sicurezza implementate per ciascun trattamento. Il registro dei trattamenti è infatti il miglior modo che ha l'organizzazione per governare in modo dinamico tutti i trattamenti che effettua sia in qualità di titolare sia in qualità di responsabile.

L'indicazione che si può trarre da questa breve analisi consiste nell'avere un approccio sistemico: l'accountability non è qualcosa che si improvvisa, ma si pianifica secondo i criteri del ciclo di Deming (Plan, Do, Check, Act – PDCA); non si tratta qui solo di rispettare un articolo di una legge secondo il vecchio modello (cosiddetto approccio cartaceo), ma è necessario adottare un approccio sistemico risk-based.