Il Sole 24 ORE

**PAESE :**Italia
**PAGINE :**13
**SUPERFICIE :**24 %
**PERIODICITÀ :**Quotidiano□□

**DIFFUSIONE :**(132114)
**AUTORE :**Aurora Agostini

► **8 aprile 2024**

# Privacy, così i modelli a misura di studio

**Protezione dei dati.** Anche nelle realtà professionali è necessario coinvolgere le figure strategiche nel percorso di allineamento al Gdpr: vanno definite la mappa delle responsabilità e dei compiti collegati ai diversi ruoli e le autorizzazioni agli accessi

*Pagina a cura di*
**Aurora Agostini**

Gli studi professionali gestiscono un'ampia gamma di dati personali (anche particolari, come quelli finanziari, giudiziari o di salute) ed è pertanto fondamentale che ciascuno costruisca un proprio personale percorso di conformità al Regolamento Ue 2016/679 (Gdpr).

In particolare, si tratta di definire, attraverso un organigramma privacy, la struttura e le responsabilità legate alla gestione e al trattamento dei dati personali e di raccogliere in un modello organizzativo privacy le politiche, le procedure e i controlli interni progettati per assicurare la gestione del rischio legato alla protezione dei dati.

Il processo di allineamento al Gdpr richiede non solo che le figure strategiche dell'organizzazione siano ben informate sulle regole di protezione dei dati personali adottate dallo studio, ma anche che siano attivamente coinvolte nella loro messa in atto. Strutturare una gestione privacy chiara e ben definita è fondamentale per proteggere i dati e per rafforzare l'integrità e la reputazione dello studio professionale.

## Organigramma privacy

L'organigramma privacy rappresenta la spina dorsale del sistema di gestione dei dati personali in uno studio professionale. Consiste infatti in una mappa dettagliata delle responsabilità e dei compiti collegati a ciascuna figura dello studio: dal responsabile della protezione dei dati (Dpo), se necessario, ai membri del personale con compiti specifici nella privacy sotto la direzione del titolare (i cosiddetti incaricati o autorizzati). Questa struttura chiave non solo precisa i vari livelli di responsabilità in linea con il Gdpr e la normativa nazionale, ma facilita anche un'efficace politica di privacy.

Anche se non è obbligatorio che questi ruoli siano coperti dai vertici dello studio, il loro coinvolgimento è riconosciuto come cruciale per la struttura privacy dell'organizzazione (articolo 29 Gdpr e articolo 2-quaterdecies del decreto legislativo 196/2003).

L'organigramma privacy dovrebbe essere rappresentato in modo grafico, per schematizzare in modo semplice e immediato le gerarchie e le linee di comando all'interno dello studio, migliorando i flussi di comunicazione interna e permettendo a tutti i membri dello staff di identificare rapidamente i referenti per le questioni di privacy e di reagire prontamente in caso di incidenti relativi ai dati.

## Autorizzazioni

Le autorizzazioni sono essenziali per mantenere la sicurezza dei dati all'interno dello studio professionale. Partendo dall'organigramma privacy, le autorizzazioni devono essere assegnate quando si presenta una necessità di accesso (anche minima), e devono contenere istruzioni precise sul trattamento dei dati indicando dettagliatamente ai dipendenti:

- il tipo di dati personali ai quali è consentito loro di accedere;
- la durata del trattamento (solitamente coincidente con la durata del rapporto lavorativo);
- la natura e la finalità del trattamento (individuata in funzione del ruolo operativo ricoperto dall'incaricato all'interno dello studio);

Il Sole 24 ORE

**PAESE :**Italia
**PAGINE :**13
**SUPERFICIE :**24 %
**PERIODICITÀ :**Quotidiano□□

**DIFFUSIONE :**(132114)
**AUTORE :**Aurora Agostini

► **8 aprile 2024**

● gli obblighi dell'incaricato (come rispetto delle istruzioni ricevute dal titolare, adozione delle misure tecniche e organizzative predisposte dal titolare, informativa e collaborazione con il titolare).

Benché il Gdpr non richieda specifiche formalità, la documentazione scritta dell'autorizzazione dei dipendenti al trattamento dei dati al momento dell'assunzione (con lettera di autorizzazione o nomina a incaricato) è il metodo migliore per provare che sono state fornite le istruzioni adeguate.

**Modello organizzativo privacy**

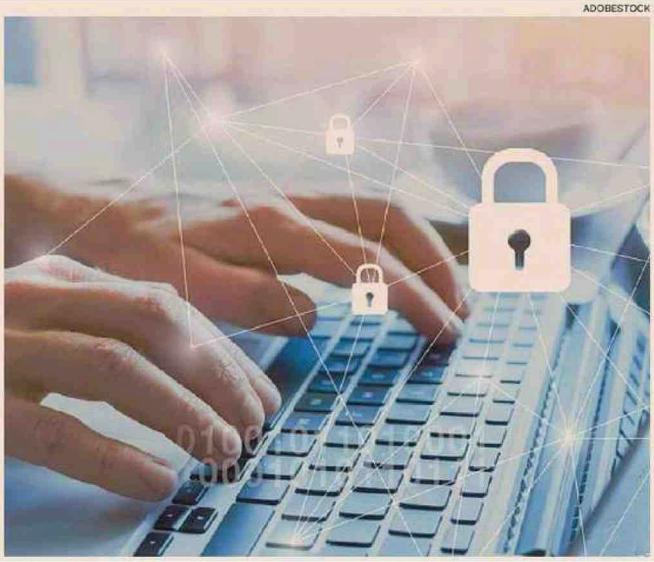
Organigramma e autorizzazioni possono essere raggruppate all'interno di un modello organizzativo privacy (Mop), ossia un framework che include e sintetizza politiche, procedure e controlli interni progettati per garantire la protezione dei dati personali.

Questo modello deve essere personalizzato per rispecchiare le specificità dello studio professionale, includendo le dimensioni dello studio, il tipo di dati trattati, i rischi associati e le misure tecniche e organizzative adottate per mitigare tali rischi. Un Mop efficace non solo aiuta a garantire la conformità normativa (è senza dubbio un atto di accountability, che consente di dimostrare più facilmente che lo studio ha messo in atto le misure di conformità necessarie per le attività che svolge), ma funge anche da punto di riferimento nella stesura e nell'aggiornamento della documentazione privacy nello studio.



**I documenti organizzativi stabiliscono politiche, procedure e controlli interni per garantire la sicurezza dei dati**

ADOBESTOCK



**Reputazione.**
Una chiara e definita gestione privacy rafforza l'immagine dello studio professionale

Il Sole 24 ORE

**PAESE :**Italia
**PAGINE :**13
**SUPERFICIE :**12 %
**PERIODICITÀ :**Quotidiano□□

**DIFFUSIONE :**(132114)
**AUTORE :**N.D.

► **8 aprile 2024**

# Necessari monitoraggio e manutenzione costanti per la tutela nel tempo

## Le verifiche
### Oltre il momento iniziale

Il regolamento generale sulla protezione dei dati (Gdpr) impone una rigorosa considerazione dei processi privacy: per avvocati, commercialisti, consulenti del lavoro e le altre realtà professionali, il Gdpr non può essere una semplice procedura formale, ma è un processo dinamico che richiede un approccio proattivo e un monitoraggio costante delle procedure di trattamento dei dati personali, per garantire una protezione efficace nel tempo e anticipare le sfide poste dal progresso digitale.

La conformità al Gdpr è un processo che si sviluppa nel tempo e va oltre la semplice verifica iniziale. Questo significa che può essere necessario rivedere come sono trattati i dati personali, quali tipologie di dati vengono gestite, come sono conservati e per quanto tempo, e adattare l'organigramma (e le autorizzazioni ai trattamenti) se cambiano i compiti delle persone che li gestiscono.

Il monitoraggio solitamente avviene attraverso:

❶ procedure di audit interno che, con cadenza trimestrale/semestrale, aiutano a identificare lacune o inefficenze nelle procedure attuali e a identificare nuovi rischi;

❷ attività di formazione per i dipendenti, da organizzare almeno una volta all'anno, per garantire che tutti siano consapevoli delle proprie responsabilità nel trattamento dei dati;

❸ un esame attento dei fornitori e dei terzi che possono trattare i dati per conto dello studio;

❹ la valutazione delle conseguenze di una violazione dei dati, non solo in termini di sanzioni, ma anche per quanto riguarda la reputazione dell'organizzazione, la fiducia dei clienti e le implicazioni a lungo termine.

Vi sono poi eventi che impongono un aggiornamento particolare, che dovrà essere implementato senza ritardo: si pensi all'acquisizione o incorporazione di altri studi, o ristrutturazioni interne che introducono nuovi servizi o modificano i processi esistenti, oppure ancora nel caso di nuove leggi, regolamenti o linee guida in materia di protezione dei dati personali.

Ma quali sono le conseguenze legate alla violazione del Gdpr? È il regolamento stesso a sottolineare la gravità di un approccio non diligente alla protezione dei dati personali, prevedendo pene pecuniarie che possono gravare in modo significativo sulle risorse economiche di uno studio professionale (le sanzioni possono raggiungere fino a 20 milioni di euro o il 4% del fatturato globale annuo). Ma tali cifre non esauriscono il quadro delle potenziali ripercussioni: la responsabilità per la violazione (ad esempio, una perdita di dati o una violazione diffusa) può tradursi anche in azioni di natura penale e avere un impatto negativo sulla percezione esterna dell'organizzazione, minando il rapporto di fiducia con la clientela e macchiando l'immagine dello studio nel lungo periodo.

Il Sole 24 ORE

**PAESE :**Italia
**PAGINE :**13
**SUPERFICIE :**12 %
**PERIODICITÀ :**Quotidiano□□

**DIFFUSIONE :**(132114)
**AUTORE :**N.D.

► **8 aprile 2024**

Da qui l'indispensabilità di un processo di revisione e aggiornamento continuo delle procedure relative al Gdpr, per assicurare conformità legale e tutelare la reputazione dell'organizzazione.