LO STUDIO DEL CONSULENTE DEL LAVORO

GDPR - CYBER SICUREZZA - LEGAL

News CDL

AUTORIZZAZIONE AL TRATTAMENTO DEI DATI

SINERGIA RISK MANAGEMENT

2023

"I soggetti autorizzati al trattamento dei dati personali"

La formazione dei dipendenti è un aspetto fondamentale per garantire la protezione dei dati personali. L'errore umano, a livello statistico, rappresenta la prima e principale causa delle violazioni dei dati personali.

Per questo motivo, è importante che le organizzazioni formino adeguatamente i propri dipendenti, in modo da sensibilizzarli sui rischi connessi al trattamento dei dati personali e sulle misure di protezione.

Ecco alcune strategie per garantire una efficace organizzazione del lavoro ed una adeguata formazione efficace dei dipendenti per la protezione dei dati personali:

1. **Identificare** i dipendenti che hanno accesso ai dati personali e definire le loro responsabilità: è importante che ogni dipendente che ha accesso ai dati personali sia consapevole dei rischi connessi al loro trattamento e delle regole da seguire per proteggerli.
2. **Fornire formazione** iniziale e aggiornamenti regolari: la formazione deve essere fornita non solo al momento dell'assunzione, ma anche con regolarità per garantire che i dipendenti siano costantemente informati sulle nuove normative e sui nuovi rischi.
3. **Coinvolgere** i dipendenti in esercitazioni pratiche: le esercitazioni pratiche possono aiutare i dipendenti a comprendere meglio le procedure e a rendersi conto dei rischi connessi al trattamento dei dati personali.
4. **Utilizzare** strumenti didattici interattivi: l'uso di strumenti didattici interattivi come quiz, giochi e video può rendere la formazione più coinvolgente e interessante per i dipendenti.
5. **Sensibilizzare** i dipendenti sui rischi connessi all'utilizzo di dispositivi personali per il lavoro: sempre più dipendenti utilizzano i propri dispositivi personali per svolgere il lavoro. È importante che i dipendenti siano consapevoli dei rischi connessi a questa pratica e siano istruiti su come utilizzare questi dispositivi in modo sicuro.

Il mancato investimento nella formazione dei dipendenti può comportare numerosi rischi per l'organizzazione, tra cui:

- **Violazione** delle normative sulla protezione dei dati personali, con conseguenti sanzioni e perdita di reputazione per l'organizzazione.

- **Perdita** o compromissione dei dati personali degli utenti, con conseguente rischio di furto di identità, frodi finanziarie e danni reputazionali per l'organizzazione.
- **Danno** alla reputazione dell'organizzazione: una violazione della sicurezza dei dati personali può compromettere la fiducia degli utenti nell'organizzazione e danneggiare la sua reputazione.

In sintesi, la formazione dei dipendenti rappresenta un passaggio fondamentale per garantire la protezione dei dati personali. È importante che le organizzazioni forniscono una formazione adeguata e regolare ai propri dipendenti, utilizzando strategie efficaci per sensibilizzarli sui rischi connessi al trattamento dei dati personali e sulle modalità di prevenzione.

La formazione costituisce un obbligo ai sensi del GDPR? Non vi è dubbio di sì.

E non solo perché la presenza della formazione nel sistema costruito dal GDPR è consacrata in alcune norme quale ad esempio l'art. 39 che afferma la **necessità di una formazione** e, ancor più, di una sensibilizzazione del personale autorizzato ad operare trattamenti. che la riferiscono, a ben vedere, al solo personale impiegato.

Ragionando più in generale è chiaro come il principio di accountability – quale metro e misura di ogni intervento posto a carico del Titolare – determini la necessità che il trattamento di dati personali avvenga previa adeguata (e all'occorrenza aggiornata) formazione in materia.

Diventa indispensabile individuare i collaboratori idonei a ricevere la delega della responsabilità di attività lavorative e professionali comportanti il trattamento anche occasionale di dati personali.

I dipendenti correttamente formati ed istruiti, in relazione alle attività correlate all'incarico attribuito, debbono porre in essere tutte le azioni necessarie a garantire che i trattamenti di dati personali effettuati avvengano nel rispetto delle disposizioni normative vigenti in materia di trattamento dei dati, compreso il profilo relativo alla sicurezza, e delle disposizioni aziendali.

In questa ottica risulta fondamentale provvedere ad autorizzare ed istruire il personale in conformità all'articolo 32 paragrafo 4 del GDPR.

Qualsiasi persona che abbia accesso ai dati personali di cui il professionista è titolare o responsabile deve avere ruoli e responsabilità definite e documentate, e deve essere costantemente aggiornata sulle modalità di trattamento e sulle regole di comportamento da seguire.

La nomina della persona autorizzata al trattamento deve essere effettuata in forma scritta e deve includere i nominativi e i relativi compiti affidati, nonché un richiamo degli obblighi generali inerenti alle misure di sicurezza per la tutela dei dati che dovranno essere trattati. Le istruzioni dettagliate da seguire nelle attività di trattamento svolte sotto l'autorità del professionista possono essere contenute all'interno di una specifica procedura che definisca le modalità di gestione e trattamento dei dati all'interno dello Studio, consegnata all'autorizzato contestualmente all'atto di designazione.

La nomina di una persona autorizzata al trattamento assume un ruolo fondamentale per garantire la sicurezza dei dati personali. Qualsiasi operazione svolta dai dipendenti o collaboratori senza l'autorizzazione del soggetto autorizzato non può essere considerata come utilizzo interno dei dati, ma costituirà di fatto una comunicazione a terzi, con tutte le problematiche del caso. Il soggetto autorizzato al trattamento deve attenersi strettamente alle istruzioni ricevute, impegnandosi al rispetto dell'obbligo di riservatezza.

Ecco un elenco sintetico dei punti principali del processo di adeguamento al GDPR relativamente al ruolo dell'autorizzato al trattamento:

- Individuare i soggetti autorizzati al trattamento dei dati personali
- Fornire autorizzazione, istruzione e formazione ai soggetti autorizzati
- Definire ruoli e responsabilità dei soggetti autorizzati in modo documentato
- Garantire che i soggetti autorizzati agiscano sotto la diretta autorità del professionista
- Redigere la nomina della persona autorizzata al trattamento in forma scritta e dettagliata
- Sviluppare e implementare un piano di gestione delle violazioni dei dati
- Verificare regolarmente la conformità al GDPR e l'efficacia delle misure di sicurezza adottate
- Mantenere una documentazione dettagliata delle attività di trattamento dei dati personali
- Adottare una mentalità proattiva nei confronti della protezione dei dati personali.

Nell'insieme di regole di condotta ed istruzioni che il Titolare del trattamento deve fornire ai soggetti autorizzati rientra necessariamento lo sviluppo e l'implementazione di un piano di gestione delle

violazioni dei dati che definisca le modalità per identificare, valutare e notificare le violazioni dei dati personali alle autorità competenti e agli interessati interessati.

Le organizzazioni debbono essere in grado di valutare e dimostrare la propria conformità al GDPR in ogni momento nonché verificare che le misure di sicurezza adottate siano adeguate a proteggere i dati personali degli interessati in base alla natura, alla portata, al contesto e alle finalità del trattamento dei dati personali. Tali adempimenti se da un lato costituiscono un obbligo del Titolare dall'altro sul piano pratico chiamano in causa l'operato dei singoli componenti l'organizzazione che debbono porre in essere ovvero mettere a terra le politiche e procedure interne predisposte per la tutela dei dati personali.

Come detto le organizzazioni hanno l'obbligo di poter dimostrare la propria compliance al Regolamento e per far ciò risulta essenziale il predisporre e conservare una documentazione dettagliata delle attività di trattamento dei dati personali, con particolare riferimento alle basi giuridiche per il trattamento dei dati, alle finalità del trattamento, alle categorie di dati personali trattati, ai destinatari dei dati personali ed alle misure di sicurezza adottate.

La documentazione deve essere facilmente accessibile e disponibile alle autorità competenti in caso di richiesta.

Nella tabella, qui di seguito, abbiamo sintetizzato i principali adempimento per un adeguamento normativo corretto.

Punto	Descrizione	Rischio
1	Individuazione dei dati personali trattati e delle basi giuridiche	Inadeguatezza della base giuridica per il trattamento dei dati personali
2	Valutazione dei rischi e dell'impatto sulla protezione dei dati (DPIA)	Rischi non valutati o non adeguatamente gestiti per la protezione dei dati personali
3	Nomina della persona autorizzata e dei responsabili al trattamento dei dati personali	Utilizzo non autorizzato dei dati personali

4	Gestione delle violazioni della sicurezza dei dati	Inadeguata gestione delle violazioni della sicurezza dei dati personali
5	Verifica periodica della conformità al GDPR	Non conformità al GDPR e rischio di sanzioni
6	Documentazione delle attività di trattamento dei dati personali	Difficoltà nell'individuazione e nella documentazione delle attività di trattamento dei dati personali

È importante sottolineare che i rischi associati a ciascun punto possono variare in base alla specifica situazione dell'organizzazione e alle caratteristiche dei dati personali trattati.

In sintesi, la protezione dei dati personali degli interessati richiede una combinazione di misure tecniche, organizzative e procedurali.

Le organizzazioni devono adottare una mentalità proattiva nei confronti della protezione dei dati personali, garantendo una formazione adeguata ai dipendenti, l'adozione di politiche e procedure interne chiare e coerenti, l'implementazione di misure di sicurezza tecniche e organizzative appropriate, e la capacità di gestire efficacemente eventuali violazioni dei dati personali.