Vademecum
I 5 step per impostare correttamente un piano di conformità al GDPR

In questo piccolo vademecum vogliamo indicare sinteticamente quali sono i 5 passi preliminari da compiere per predisporre la conformità delle procedure aziendali al GDPR.

Questo vademecum può essere utilizzato dal **Titolare del Trattamento dei Dati** come una veloce guida e come promemoria sui passi da compiere e sulle verifiche che deve effettuare.

Verificare se l'Ente o l'azienda sono soggetti agli obblighi previsti dal GDPR

In particolare sono soggetti al GDPR gli Enti le aziende che effettuano trattamenti di dati personali.

Cosa si intende per trattamento?
Si intende con tale definizione "qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati".

Cosa si intende per dati personali?
Per "dato personale" si deve intendere "qualunque informazione relativa a persona fisica identificata o identificabile anche indirettamente mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".
Quindi in definitiva se l'azienda - caso altamente improbabile - non effettua alcun trattamento di dati personali non deve sottostare agli obblighi previsti dal GDPR.

Mappatura di tutti i dati personali e dei trattamenti che vengono effettuati su tali dati.

Particolari cautele organizzative e gestionali richiederanno i seguenti tipi di dati personali:

a) i dati personali idonei a rivelare l'origine razziale ed etnica
b) i dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere passibile di discriminazione
c) i dati personali idonei a rivelare le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
d) i dati personali idonei a rivelare lo stato di salute e la vita sessuale

e) I dati biometrici, intendendosi con tali i dati ottenuti da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca
f) I dati giudiziari intendendosi con tali i dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Andranno altresì tenuti in debita considerazione anche quei dati che non rientrano nelle categorie sopra indicate, ma il cui trattamento presenta rischi specifici per i diritti e le libertà fondamentali ovvero per la dignità dell'interessato.
Si pensa in primo luogo ai dati patrimoniali (es: dichiarazione dei redditi), ma, più in generale, ad ogni dato personale il cui trattamento potrebbe potenzialmente ledere la dignità della persona o la sua riservatezza (si pensi, ad esempio, alla divulgazione di particolari immagini, foto o video).

Suggerimento

Il Titolare del Trattamento dei dati verifichi insieme al DPO se è stato istituito correttamente il Registro dei Trattamenti.

Valutare, per ogni tipologia di dato raccolto, se il trattamento effettuato è legittimo

In particolare ricordiamo che il trattamento di un dato personale è legittimo, ai sensi dell'articolo 6 del GDPR solo se ricorre una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Suggerimento

Il Titolare del Trattamento dei dati verifichi insieme al DPO se sono state predisposte le corrette informative.

Valutare l'esistenza e la validità di tutti i presidi previsti dalla normativa GDPR

In particolare i principali presidi sono i seguenti:

- individuazione del titolare del trattamento dati, ovvero del soggetto che presiede ai suddetti trattamenti
- verifica della nomina di eventuali figure delegate e della relativa formalizzazione di tale nomina; in particolare ci si riferisce alle seguenti figure:
  - responsabile trattamento dati
  - soggetti che effettuano attività di trattamento dei dati aziendali in outsourcing (es: commercialista, studio paghe)
  - Data protection Officer (DPO)
- verifica dell'acquisizione del consenso da parte dell'interessato e del rilascio allo stesso dell'informativa per il trattamento dei dati personali; in particolare l'informativa rilasciata a partire dal 25 maggio 2018 deve essere conforme al GDPR, quindi occorrerà rivedere le vecchie informative utilizzate
- verifica esistenza misure adeguate di sicurezza sia per gli archivi fisici che per gli archivi informatici

Suggerimento

Il Titolare del Trattamento dei dati verifichi insieme al DPO e all'Amministratore di Sistema se sono state approntate le corrette misure adeguate di sicurezza e se sono state predisposte le corrette informative.

Considerare, laddove possibile, tutte gli accorgimenti, sia a livello organizzativo che a livello informatico, che consentono la limitazione dell'impatto del GDPR

Tali accorgimenti possono consentire di ridurre l'impegno dell'impresa sia per l'adeguamento al GDPR sia per il mantenimento della conformità.
A titolo esemplificativo l'Ente o l'azienda potrà:

- ridurre il numero dei campi per i dati personali raccolti o elaborati
- ridurre la quantità di tempo per cui i dati personali vengono conservati o elaborati
- crittografare i dati durante la memorizzazione e la trasmissione
- nascondere gli indirizzi ip e rendere anonimi altri tipi di informazione utente
- ridurre il numero di persone autorizzate ad accedere ai dati personali
- aumentare la capacità di prevenire e correggere le minacce che mirano a colpire i dati personali.

Suggerimento

Il Titolare del Trattamento dei dati discuta insieme al DPO degli accorgimenti tecnici e amministrativi per minimizzare gli effetti del GDPR sulle pratiche quotidiane di trattamento dei dati.

