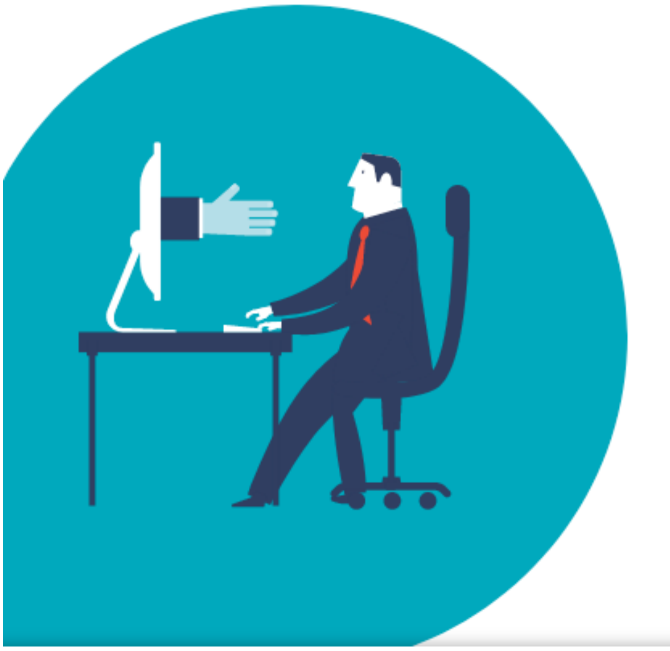
PRIVACY E DPO



AUDIT IN MATERIA DI **PRIVACY**

Svolgere delle verifiche in ambito privacy è molto complesso e richiede competenze molteplici, specialistiche ed una grande esperienza che non si può improvvisare. Anche per questo motivo diventa fondamentale affidarsi ad un esperto.

Ma procediamo con ordine.

Cosa si intende per auditing?

Uno step fondamentale ed imprescindibile in ambito privacy è l'audit che consiste in una valutazione di conformità dell'azienda/ente, sotto il profilo del trattamento dei dati personali.

Attraverso di esso vengono messe in rilievo le eventuali criticità da correggere all'interno dell'azienda/ente, andando così ad analizzare tutta la parte relativa alla documentazione, al flusso di dati personali dell'azienda, in modo da misurare la rispondenza o meno della situazione e delle policy aziendali in ambito privacy.

In cosa consiste un audit privacy? E quali sono i passaggi da seguire?

1) Analizzare il modello organizzativo dell'azienda. Compito del DPO è anzitutto valutare ed esaminare il modello organizzativo dell'azienda o dell'ente. In settori particolarmente normati, come ad esempio quello bancario/finanziario, il modello organizzativo è definito dalle indicazioni della Banca d'Italia. In tal ipotesi il DPO verificherà il rispetto dell'organizzazione aziendale al modello normativo. Negli altri casi invece, il DPO assumerà, come modello di riferimento, la normativa "base" in materia di privacy e effettuerà verifiche e approfondimenti, volti ad accertare a che punto sono gli eventuali *remediation plan,* o a suggerire un suo *remediation plan,* sulla base di carenze rilevate dalla documentazione.

"Perchè affidarsi ad un DPO? "

"La verifica di conformità di un'azienda e/o di ente è un'operazione complessa che necessita del supporto di un esperto"

2) Fare il piano di audit preferibilmente triennale. Il DPO dovrà proporre e concordare con l'azienda un piano audit, meglio se triennale, tempo minimo per effettuare i diversi controlli e alla fine poter tornare su settori già controllati o ampliare lo *scope*.

Nella definizione del piano di audit e nelle fasi successive sarà vincente la disponibilità di un team interdisciplinare, in grado di mettere in campo diverse professionalità, come quelle di tipo legale, organizzativo e di sicurezza. Fondamentale è la collaborazione Team DPO - Team Aziendale/Amministrativo.

3) Formulare un piano coerente con il tipo di azienda e i trattamenti rilevanti. Il DPO procede a predisporre controlli trasversali e verticali, sui reparti ed uffici, diversi per ogni settore.

4) Predisporre una check list. Per ogni controllo il DPO definisce una lista di controlli condivisa con l'azienda/ente e coerente con il tipo di audit.

5) Raccogliere evidenze ed esempi durante l'audit. La raccolta di dati ed esempi, puntualmente riferiti ai diversi punti della check list, andranno allegati al report finale. Nel caso di verifica della gestione dei fornitori, ad esempio, il DPO dovrà estrarre la lista di quelli che trattano dati personali, selezionare esempi significativi, verificare i contratti e le nomine a Responsabile.

6) Audit report, remediation plan e follow-up. Il Dpo redige l'audit report. Dopo di che, altrettanto importante è il remediation plan che suggerisca le misure da adottare per mitigare la non conformità, ne indica le priorità e una data entro la quale devono essere adottate. Fondamentale infine il follow-up, che deve essere previsto fin dall'inizio e puntualmente eseguito.

Un audit report e un *remediation plan* chiusi in un cassetto, senza una verifica della loro attuazione, sono inutili. Il controllo sulla conformità del *remedation plan* viene fatto periodicamente. **L'attività del DPO, quindi, non si esaurisce alla realizzazione del planning, ma si estende al controllo e alla verifica periodica del rispetto della normativa da parte dell'ente o dell'azienda.**

Perché fare un audit?

Attraverso l'audit è possibile far emergere le debolezze dell'organizzazione e quindi individuare delle soluzioni correttive. Perlomeno in superficie, lo scopo principale dell'audit aziendale è quello di rispettare le procedure predisposte e quindi di adempiere agli obblighi normativi.

Chi può fare audit?

La complessità delle operazioni sopra descritte rende chiaro che questo tipo di attività va effettuata ad opera di un esperto. Il nostro Team è in grado di accompagnarti in questi passaggi e realizzare per te o la tua azienda un piano "privacy" adatto a tutte le esigenze e rispettoso della normativa in materia.

Verifica dei Documenti in tuo possesso - Audit Documentazione

Tra le più importanti attività che il Team di Data Protection può svolgere per un'azienda/ente vi è la verifica della documentazione aziendale/amministrativa.

Il Regolamento Europeo sulla Privacy impone svariati obblighi e doveri alle aziende/enti che si trovino a dover trattare i dati personali dei residenti dell'Unione Europea. Tra questi vi è **l'utilizzo di documentazione amministrativa/aziendale che risulti in linea con la normativa GDPR** e le altre disposizioni nazionali o dell'Unione relative alla protezione dei dati.

In tal senso, il supporto di un DPO può risultare fondamentale.

Ad es. senza l'operato di un DPO certificato è possibile che alcuni documenti aziendali – prodotti da fornitori esterni – non siano esattamente a norma GDPR con il rischio, per l'azienda, di incappare in pesanti sanzioni.

Spesso, infatti, i fornitori fanno firmare alle aziende-clienti dei documenti che risultano imprecisi, impropri e che in molti casi, sono stati copiati, senza troppa attenzione, da un contenuto presente sul web, dopo una frettolosa ricerca su Google.

Questo pone chiaramente un problema per l'Azienda, che in realtà dovrebbe sempre controllare la correttezza formale di quei documenti, ma spesso non ha né il tempo, né le competenze interne per poterli verificare.

Con il servizio di **Audit della Documentazione** diamo la possibilità, a tutte le aziende/enti interessati di far controllare da una società esterna l'accuratezza e la conformità dei documenti in possesso dell'azienda. In altre parole un nostro DPO verificherà contratti, nomine, registro dei trattamenti, registro della violazioni dei dati ecc.

Con il nostro servizio, hai la certezza di affidarti a personale esperto e competente, che saprà valutare la documentazione aziendale, indicandoti eventuali criticità, inesattezze, aiutandoti ad allinearti agli adempimenti del GDPR.