SicurAzienda Blog

SEGRETERIA@SICURAZIENDA.COM
WWW.SICURAZIENDA.COM

SocialWall

6 GIUGNO 2024

Audit di seconda parte dei responsabili del trattamento Gestione dati conforme al GDPR

L'audit al responsabile del trattamento è un'attività regolamentata dall'Articolo 28 del Regolamento Generale sulla Protezione dei Dati (GDPR).

Il servizio che SicurAzienda propone è di consulenza e/o espletamento delle attività di audit di seconda parte. Questi audit, **noti anche come audit di seconda parte**, si suddividono in diverse categorie:

- **Audit di pre-qualifica**: questi audit vengono condotti prima della sottoscrizione del contratto (azienda fornitrice del servizio), tra il titolare del trattamento e il responsabile (DPO). Durante questa fase, il titolare ha l'opportunità di presentare la propria organizzazione e comunicare le proprie esigenze.
  È un momento per stabilire una base di comprensione reciproca e definire l le aspettative.

- **Audit di mantenimento o audit di seconda parte**: questi avvengono dopo la sottoscrizione del contratto e durante la fornitura di servizi negli anni successivi (auditor).
  Durante un audit di mantenimento, il titolare può condividere i risultati delle prestazioni con il responsabile (DPO) e discutere delle future esigenze.

- **Audit congiunti**: In alcuni casi, il titolare può richiedere un audit congiunto con il responsabile (DPO) presso un soggetto terzo (sub-responsabile) che tratta dati del titolare su mandato del responsabile. Questo tipo di audit è utile per valutare la conformità di tutti i soggetti coinvolti nel trattamento dei dati.

Cosa succede se vengono rilevate violazioni durante l'audit?

Durante un audit al responsabile del trattamento, se vengono rilevate violazioni o non conformità, è importante seguire alcune procedure:

Identificazione delle violazioni: l'auditor deve documentare accuratamente le violazioni o le aree di non conformità riscontrate durante l'audit.
Questo può includere problemi come la mancata adozione di misure di sicurezza adeguate, la mancanza di documentazione o la gestione inappropriata dei dati personali.

Comunicazione con il responsabile: l'auditor dovrebbe comunicare immediatamente le violazioni al responsabile del trattamento. Questo può avvenire tramite un rapporto scritto o una riunione di feedback. Durante questa comunicazione, è importante fornire dettagli specifici sulle violazioni riscontrate.

Pianificazione delle azioni correttive: il responsabile del trattamento dovrebbe avviare azioni correttive per risolvere le violazioni. Questo può includere la revisione delle procedure, l'aggiornamento della documentazione, la formazione del personale o altre misure adeguate.

Monitoraggio e follow-up: dopo aver implementato le azioni correttive, è importante monitorare continuamente la conformità del responsabile del trattamento. L'auditor può pianificare un follow-up per verificare che le correzioni siano state effettuate e che le violazioni siano state risolte.

Segnalazione alle autorità di controllo: in alcuni casi, se le violazioni sono gravi o persistenti, l'auditor potrebbe dover segnalare il caso alle autorità di controllo competenti. Queste autorità possono prendere ulteriori misure, come l'imposizione di sanzioni o l'avvio di indagini.

Qual è il ruolo del Data Protection Officer (DPO) nell'audit del responsabile del trattamento?

**Il Data Protection Officer (DPO), o Responsabile della Protezione dei Dati, è una figura chiave nell'ambito della protezione dei dati personali.
Vediamo quali sono i suoi ruoli e responsabilità specifici nell'audit del responsabile del trattamento:**

Informare e fornire consulenza al titolare del trattamento: il DPO è responsabile di informare il titolare del trattamento riguardo alle normative GDPR e altre disposizioni relative alla protezione dei dati. Inoltre, fornisce consulenza su come garantire la conformità alle leggi sulla privacy e sulla gestione corretta dei dati personali.

Sorvegliare la conformità: il DPO monitora attentamente l'osservanza delle norme GDPR e delle altre disposizioni nazionali o dell'Unione relative alla protezione dei dati. Questo ruolo di supervisione è fondamentale per garantire che l'azienda rispetti le leggi sulla privacy e protegga i dati dei soggetti interessati.

Valutazione d'impatto (DPIA): quando richiesto, il DPO fornisce un parere sulla valutazione d'impatto sulla protezione dei dati (DPIA). Questa valutazione è un processo che aiuta a identificare e mitigare i rischi associati al trattamento dei dati personali. Il DPO contribuisce a garantire che le DPIA siano condotte in modo accurato e completo.