1. GARANZIA

Il RGDP raccomanda l'uso di schemi di certificazione come ISO 27001 per fornire la garanzia necessaria che l'azienda sta gestendo i rischi per la sicurezza delle informazioni in modo efficace.

2. NON SOLO DATI PERSONALI

ISO 27001 segue le best practice internazionali e ti aiuterà a mettere in atto processi che proteggono non solo le informazioni sui tuoi clienti ma anche tutte le altre risorse informative in qualsiasi forma, dalle informazioni archiviate elettronicamente a quelle in formato cartaceo.

3. QUADRO DI CONTROLLO E DI SICUREZZA

Il RGPD stabilisce che le aziende devono selezionare controlli tecnici e organizzativi adeguati per mitigare i rischi identificati. La maggior parte delle disposizioni e dei controlli sulla protezione dei dati stabiliti dal RGPD sono raccomandati anche dall'ISO 27001.

9 MODI CON CUI ISO 27001 TI AIUTA A CONFORMARTI AL RGPD

ISO 27001 è uno standard di gestione della sicurezza delle informazioni che fornisce indicazioni dettagliate per adottare misure di sicurezza appropriate sotto forma di un sistema di gestione della sicurezza delle informazioni (SGSI), per proteggere l'azienda da una violazione dei dati.

Un SGSI è un insieme di processi, documenti, tecnologia e persone che aiuta a gestire, monitorare, controllare e migliorare le pratiche di sicurezza delle informazioni dell'organizzazione. Ti aiuta a gestire tutti i tuoi sistemi di sicurezza in un unico posto, in modo coerente ed economico.

Piuttosto che implementare controlli in modo indiscriminato per ridurre il rischio di violazione dei dati, seguendo uno standard di sicurezza delle informazioni, sarai in grado di implementare misure di sicurezza adeguate ed efficaci, basate sui risultati di una valutazione formale del rischio, in conformità del RGPD.

Ecco qui i 9 modi con i quali ISO 27001 ti aiuta a conformarti al RGPD.

4. PERSONE, PROCESSI E TECNOLOGIA

ISO 27001 comprende i tre aspetti essenziali della sicurezza delle informazioni: persone, processi e tecnologia, il che significa che puoi proteggere la tua attività non solo da rischi tecnologici ma anche da altre minacce più comuni, come il personale poco informato o procedure inefficaci.

9. CERTIFICAZIONE

Il RGPD richiede alle organizzazioni di adottare le misure necessarie per garantire che i controlli di sicurezza funzionino come previsto. Il conseguimento della certificazione accreditata ISO 27001 offre una valutazione indipendente ed esperta in merito alla possibilità di implementare misure adeguate alla protezione dei dati.

L'implementazione di un SGSI conforme all'ISO 27001 non è solo una best practice per la sicurezza delle informazioni, ma è anche parte integrante per dimostrare la conformità alla protezione dei dati.
Leggi ulteriori informazioni sull'ISO 27001.

Scopri come iniziare parlando con uno dei nostri esperti.

5. RESPONSABILITA'

ISO 27001 richiede che il tuo regime di sicurezza sia supportato dalla top leadership e incorporato nella cultura e nella strategia dell'organizzazione. Inoltre, richiede la nomina di un membro senior che si assuma la responsabilità del SGSI. A sua volta, il RGPD richiede una chiara responsabilità per la protezione dei dati in tutta l'organizzazione.

8. TEST E AUDIT

Essere conforme al RGPD significa che l'azienda deve eseguire test e verifiche a scadenza regolare per dimostrare che il suo regime di sicurezza funzioni in modo efficace. Un SGSI conforme all'ISO 27001 deve essere valutato ad intervalli regolari in base alle linee guida di audit interno fornite dallo Standard.

7. MIGLIORAMENTO CONTINUO

ISO 27001 richiede che il tuo SGSI sia costantemente monitorato, aggiornato e revisionato, in modo tale che si evolva man mano che la tua attività evolve, con un processo di miglioramento continuo. Ciò significa che il tuo SGSI si adatterà ai cambiamenti – sia interni che esterni – man mano che tu identifichi e riduci i rischi.

6. VALUTAZIONE DEL RISCHIO

La conformità all'ISO 27001 significa condurre valutazioni periodiche del rischio per identificare minacce e vulnerabilità che possono influenzare il patrimonio delle informazioni, ed adottare misure per proteggere tali dati. Il RGPD richiede specificatamente una valutazione del rischio per garantire che un'organizzazione abbia identificato i rischi che possono avere un impatto sui dati personali.