

CERTIFICAZIONE BS 10012:2017

Data Protection – Sistema di
Gestione Dati Personali



DESTINATARI

Il servizio è rivolto a tutte le organizzazioni che vogliono garantire e dare evidenza della compliance aziendale alla normativa Nazionale ed Europea in tema di dati personali (GDPR), mediante l'adozione di best practices riconosciute a livello internazionale.

IL CONTESTO

Il 25 maggio 2018 inizierà ad avere efficacia il nuovo Regolamento UE 2016/679 (GDPR, General Data Protection Regulation).

Con questo nuovo regolamento generale sulla protezione dei dati, pubblicato su Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, la Commissione europea ha inteso rafforzare e rendere più omogenea la protezione dei dati personali dei cittadini e residenti dell'Unione Europea.

Dal 25 maggio 2018, il GDPR abrogherà le norme del Codice per la protezione dei dati personali (D. Lgs.n. 196/2003) che risulteranno con esso incompatibili.

La normativa prescrive le regole per la gestione dei dati personali a livello nazionale e al di fuori dell'UE, la cui osservanza ricade su tutti i Titolari del trattamento dei dati (anche con sede legale fuori dall'Unione Europea) che trattano dati di residenti nell'unione europea.

Lo standard BS 10012:2017, elaborato e promosso dall'Organizzazione britannica di standardizzazione (British Standards Institution), rappresenta un valido strumento per la gestione aziendale degli aspetti organizzativi e prescrittivi previsti dalla recente normativa europea (Regolamento UE 2016/679).

IL SERVIZIO

Il servizio di Certificazione secondo lo standard BS 10012:2017 assicura all'Azienda l'adozione di un sistema affidabile per la gestione dei dati personali trattati, in conformità agli obblighi stabiliti dal Reg. UE 2016/679 (GDPR).

E' uno strumento per garantire alla Direzione Aziendale (Titolare del trattamento) e a terzi (privati, enti di controllo, ecc.) l'adozione di policy ed istruzioni per il corretto trattamento dei dati. La certificazione BS 10012 garantisce:

- Compliance: fornisce evidenza che la propria organizzazione soddisfa i requisiti del GDPR, dimostrandone la compliance e l'accountability.
- Gestione dei Rischi: aiuta a identificare e mitigare i rischi per la sicurezza dei dati personali trattati nei propri processi aziendali.
- Reputazione: la certificazione BS 10012 è uno strumento a salvaguardia della reputazione aziendale in relazione a possibili violazioni della sicurezza dei dati.

ITER DI CERTIFICAZIONE

Lo standard BS 10012:2017 è strutturato secondo il modello degli standard ISO (HLS - High Level Structure) per garantire la massima integrazione con i Sistemi di Gestione già certificati dall'Organizzazione, in particolare modo gli standard ISO 9001:2015 ed ISO 27001:2013.

L'iter di certificazione segue le modalità tipiche delle certificazioni dei Sistemi di Gestione:

- la richiesta di offerta (MOD DOM);
- l'accettazione dell'offerta;
- lo svolgimento di un audit di Certificazione (suddiviso in due stage);
- la gestione di eventuali carenze;
- la delibera di certificazione da parte della Commissione Tecnica Certiquality;
- lo svolgimento di verifiche di mantenimento

SERVIZIO DI GAP ASSESSMENT

Il servizio opzionale di gap assessment è un ulteriore strumento a disposizione dell'Organizzazione per identificare e comprendere le eventuali aree critiche, ad alto rischio o deboli rispetto alle prescrizioni stabilite dal GDPR. L'attività svolta dai nostri auditor consente di verificare le policy, le procedure ed i controlli in vigore in Azienda a tutela delle informazioni personali trattate.

Tale attività di audit può essere funzionale per l'Organizzazione ed i propri Responsabili per il trattamento dei dati sia in fase di primo approccio alla gestione della compliance al GDPR, a prescindere dalla volontà di implementare un sistema di gestione secondo la norma BS 10012:2017, sia in fase avanzata di implementazione di un Sistema di Gestione.

FORMAZIONE E CERTIFICAZIONE DPO (Data Protection Officer)

Certiquality integra le attività in campo con un programma di corsi di formazione a catalogo e in azienda.

Il servizio di certificazione per i DPO si basa sui criteri stabiliti dalla norma UNI 11697 «Attività professionali non regolamentate – Profili professionali relativi al trattamento e alla protezione dei dati personali – Requisiti di conoscenza, abilità e competenza», pubblicata a novembre 2017 al fine di definire i profili professionali relativi al trattamento e alla protezione dei dati personali.

