Aggiornamento ISO 27701:2025 – Cosa è cambiato e perché è importante

January 9, 2026

Le organizzazioni di tutti i settori sono sottoposte a una crescente pressione per dimostrare come proteggono i dati personali. Clienti, partner e autorità di controllo si aspettano prove verificabili di conformità e responsabilità, non soltanto procedure scritte “sulla carta”.

La ISO 27701:2025 offre esattamente questo. Come standard internazionale aggiornato per stabilire i requisiti per un sistema di gestione della riservatezza delle informazioni (Privacy Information Management Systems o PIMS), fornisce un metodo riconosciuto e verificabile per dimostrare la maturità in materia di privacy, rafforzare la governance e costruire fiducia tra gli stakeholder. Per le organizzazioni che cercano una garanzia indipendente, questo aggiornamento rappresenta un’opportunità concreta per rafforzare la fiducia nel modo in cui vengono gestiti i dati personali.

In questo blog spieghiamo cosa è cambiato nella ISO 27701:2025, perché questi aggiornamenti sono importanti per le organizzazioni e come la guida esperta di un Data Protection Officer può aiutare a tradurre lo standard in risultati concreti e misurabili.

Cosa è la ISO 27701?

La ISO 27701 è lo standard internazionale per stabilire i requisiti per un sistema di gestione della riservatezza delle informazioni (Privacy Information Management Systems o PIMS). Fornisce un quadro strutturato per gestire i dati personali in modo responsabile, dimostrare la conformità alle normative globali sulla privacy e costruire la fiducia degli stakeholder rispetto al modo in cui le organizzazioni trattano le informazioni personali.

Pubblicato per la prima volta nel 2019 come estensione della ISO 27001, lo standard ha aiutato organizzazioni di tutto il mondo a dimostrare il proprio impegno verso la privacy oltre la semplice conformità reattiva. L’edizione 2025 segna un’evoluzione significativa, rendendo la certificazione in materia di privacy più accessibile e affrontando al contempo le sfide attuali della protezione dei dati.

Cosa è cambiato nella ISO 27701:2025?

L'edizione 2025 introduce aggiornamenti significativi che riflettono l'evoluzione dei rischi legati alla privacy e delle aspettative in materia di accountability dal momento della prima pubblicazione dello standard nel 2019.

Le principali novità includono: certificazione autonoma, una nuova struttura del sistema di gestione, controlli più chiari basati sui ruoli, gestione obbligatoria del rischio privacy, una copertura più ampia delle sfide moderne e un rafforzato allineamento con le normative globali sulla privacy.

Di seguito analizziamo ciascuno di questi aggiornamenti in maggiore dettaglio, evidenziando cosa significano in pratica per le organizzazioni.

Certificazione autonoma in materia di privacy

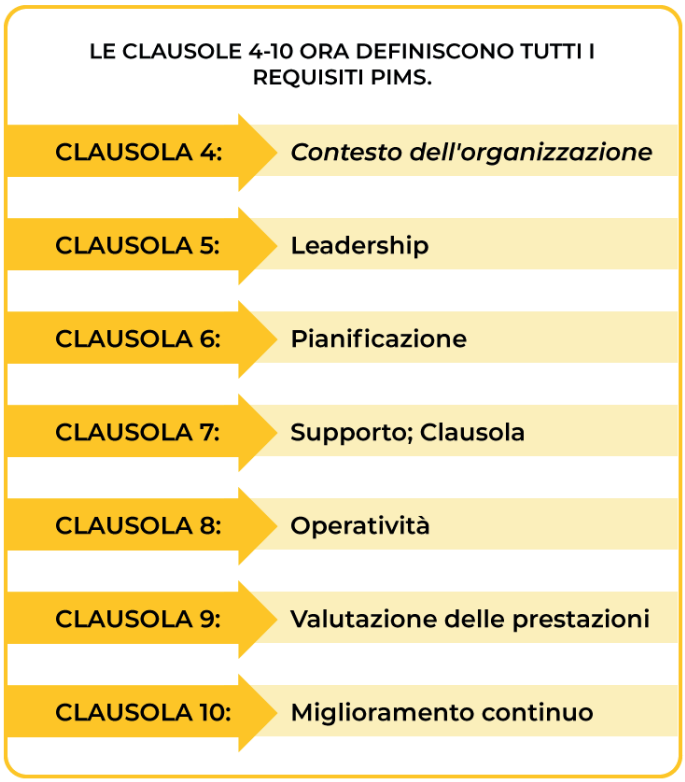
La ISO 27701:2025 può ora essere certificata indipendentemente dalla ISO 27001. Questo cambiamento riconosce la privacy come disciplina gestionale autonoma e offre alle organizzazioni un percorso diretto verso la certificazione.

Eliminando la necessità di implementare un Information Security Management System (ISMS) completo, le organizzazioni non devono più seguire prima la ISO 27001. Ciò rende la certificazione più rapida, più economica e più semplice da ottenere, in particolare per i team che necessitano di una prova credibile e verificabile dell'accountability in materia di privacy, senza i costi o la complessità di un intero framework di sicurezza.

Nuova struttura del sistema di gestione

Lo standard adotta ora la High-Level Structure (HLS) comune a tutti gli standard ISO relativi ai sistemi di gestione.

Le clausole 4–10 definiscono ora tutti i requisiti del PIMS, rendendo più semplice integrare la privacy con framework già esistenti, come ISO 9001 o ISO 14001.



Controlli più chiari basati sui ruoli

I controlli sono ora organizzati in tre categorie definite, eliminando le ambiguità tra le responsabilità di titolari e responsabili del trattamento e allineandosi più strettamente ai ruoli previsti dalle normative sulla protezione dei dati.

- **Titolari del trattamento dei dati personali (PII Controllers)**: 31 controlli per le organizzazioni che determinano le finalità e i mezzi del trattamento
- **Responsabili del trattamento (PII Processors)**: 18 controlli per le organizzazioni che trattano dati per conto dei titolari
- **Sicurezza delle informazioni**: 29 controlli applicabili a entrambi i ruoli, con un focus specifico sulla privacy

Lo standard amplia inoltre la copertura dei controlli per riflettere nuove considerazioni in materia di privacy, come i dati biometrici, la trasparenza algoritmica e i meccanismi di verifica dell'età.

Elemento di particolare rilievo: l'Allegato B, che fornisce indicazioni dettagliate per l'implementazione di ciascun controllo, è ora normativo. Ciò significa che le organizzazioni sono tenute a utilizzare tali linee guida come parte del processo di certificazione, garantendo aspettative più chiare e una valutazione più coerente dei controlli privacy in contesti differenti.

Gestione obbligatoria del rischio privacy

Nell'edizione del 2019 la gestione del rischio privacy era implicita, ma non esplicita. La ISO 27701:2025 la rende ora un requisito formale, integrando la valutazione del rischio privacy nella governance organizzativa.

Le organizzazioni devono:

- Valutare i rischi per i diritti e le libertà delle persone
- Valutare i rischi per l'organizzazione, come impatti operativi, finanziari o reputazionali
- Integrare la gestione del rischio privacy e della sicurezza delle informazioni in un approccio unificato
- Mantenere una metodologia documentata che illustri come i rischi privacy vengono identificati, valutati, trattati e monitorati all'interno dell'organizzazione

Lo standard riconosce che gli incidenti privacy possono compromettere la fiducia degli stakeholder tanto quanto le violazioni di sicurezza. Richiede pertanto alle organizzazioni di valutare minacce moderne, come il profiling basato su AI, i trasferimenti transfrontalieri di dati e gli ecosistemi Internet of Things (IoT), nell'ambito del processo formale di gestione del rischio.

Le sfide moderne della privacy

La ISO 27701:2025 amplia il proprio ambito per riflettere i rischi privacy più attuali, garantendo che lo standard rimanga in linea con le tecnologie più moderne e con le aspettative regolatorie. I requisiti di rischio aggiornati coprono:

- Profilazione basata su AI e decisioni automatizzate
- Servizi cloud e modelli di responsabilità condivisa
- Trasferimenti transfrontalieri di dati e valutazioni di adeguatezza
- Trattamento di dati biometrici e sanitari
- Dati dei minori e meccanismi di verifica dell'età
- Ambienti Internet of Things (IoT) e dispositivi connessi
- Condivisione di dati con terze parti e supervisione dei responsabili del trattamento

Allineamento globale alle normative privacy

L'edizione 2025 rafforza la propria rilevanza al di là delle normative europee. La terminologia aggiornata e le aspettative sui controlli supportano ora la conformità alle principali normative sulla privacy a livello globale, tra cui:

- UK Data Protection Act 2018
- California Consumer Privacy Act (CCPA)
- California Privacy Rights Act (CPRA)
- Brazilian General Data Protection Law (LGPD)
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Personal Data Protection Act (PDPA) di Singapore e Thailandia

Allineandosi ai requisiti internazionali, lo standard aiuta le organizzazioni a dimostrare accountability in più giurisdizioni, riducendo duplicazioni, semplificando la due diligence e supportando le operazioni globali.

Benefici della ISO 27701:2025

Per le organizzazioni che desiderano andare oltre una conformità limitata alle sole policy, la ISO 27701:2025 offre un percorso misurabile verso una maggiore maturità in materia di privacy e una garanzia operativa più solida.

Un punto di riferimento riconosciuto per l'accountability

La certificazione indipendente dimostra che la governance della privacy è strutturata, misurabile e pronta per l'audit, allineandosi alle aspettative globali in materia di accountability.

Maggiori opportunità di accesso al mercato

Poiché i clienti richiedono prove della corretta gestione dei rischi privacy, la certificazione può accelerare le procedure di onboarding, ridurre gli oneri di due diligence e favorire l'accesso a mercati regolamentati o internazionali.

Coerenza nelle operazioni di privacy

La struttura aggiornata e le linee guida obbligatorie presenti nell'Allegato B garantiscono che la privacy sia implementata in modo coerente tra team e processi, riducendo ambiguità e lacune di conformità.

Supporto alla crescita e al cambiamento

Un sistema di gestione della riservatezza delle informazioni (PIMS) scalabile consente alle organizzazioni di adattarsi con sicurezza a nuovi mercati, nuovi utilizzi dei dati, nuove tecnologie e nuovi requisiti normativi.

Evidenza di leadership e maturità culturale

La certificazione segnala che la privacy è integrata nella governance organizzativa, rafforzando la fiducia di clienti, partner e organismi di controllo.

Resilienza regolatoria

Con un allineamento più forte alle normative globali sulla privacy e con la gestione obbligatoria del rischio, le organizzazioni sono meglio preparate a sostenere verifiche regolatorie e nuove esigenze di conformità.

Chi dovrebbe guidare l'implementazione della ISO 27701?

La ISO 27701:2025 introduce aspettative più chiare in materia di accountability, governance e gestione del rischio privacy. Soddisfare tali aspettative richiede una comprensione approfondita di come i dati personali vengono trattati, protetti e governati all'interno dell'organizzazione.

È qui che il Data Protection Officer (DPO) apporta un valore unico. Con la guida del DPO, la certificazione diventa un modo per dimostrare una governance privacy significativa, non semplicemente per produrre documentazione a fini di audit.

Un DPO offre:

- **Supervisione legale e operativa**: garantisce che i controlli riflettano i requisiti normativi e le esigenze operative reali, riducendo il rischio di interpretazioni errate.
- **Visibilità end-to-end sui flussi di dati**: comprende come i dati si muovono tra team e sistemi, elemento essenziale per mappare rischi e ruoli rispetto ai controlli specifici.
- **Autorità per consolidare l'accountability**: promuove l'adozione e la conformità a livello organizzativo.
- **Integrazione tra privacy e sicurezza**: aiuta ad allineare il PIMS alle strutture operative e di sicurezza esistenti, evitando duplicazioni e priorità contrastanti.

The DPO Centre ha esperienza nell'aiutare le organizzazioni a dimostrare accountability in materia di privacy attraverso la conformità alla ISO/IEC 27701. Contattaci per discutere come possiamo supportarti nella preparazione e nell'implementazione con sicurezza.

Frequently asked questions

Le organizzazioni devono avere la ISO 27001 per ottenere la certificazione ISO 27701?

No, la ISO 27701:2025 può essere certificata indipendentemente dalla ISO 27001. Le organizzazioni che dispongono già di un sistema di gestione della sicurezza informatica (Information Security Management System o ISMS) possono comunque integrare entrambi gli standard, ma non è più un prerequisito per dimostrare la maturità in materia di privacy.

In che modo la ISO 27701 supporta la conformità al GDPR?

Lo standard fornisce un quadro strutturato per dimostrare l'accountability, includendo governance, definizioni di ruolo, gestione del rischio e controlli di protezione dei dati allineati ai principi del GDPR. Sebbene la certificazione non garantisca automaticamente la conformità al GDPR, offre ad auditor, clienti e autorità una garanzia oggettiva che gli obblighi chiave siano integrati nelle operazioni.

La certificazione ISO 27701 è obbligatoria?

No, la certificazione è volontaria, ma sempre più riconosciuta come best practice. Ottenerla dimostra un impegno proattivo verso la privacy e offre garanzie a regolatori, clienti e partner sul fatto che la protezione dei dati è considerata con serietà.

Cosa devo fare se sono già certificato ISO 27701:2019?

È previsto un periodo di transizione formale fino a ottobre 2028. Le organizzazioni dovranno aggiornare il proprio sistema di gestione delle informazioni sulla privacy per riflettere le modifiche introdotte nell'edizione 2025, inclusa la nuova struttura, i controlli aggiornati e la gestione obbligatoria del rischio privacy. La transizione avviene solitamente durante il successivo ciclo di audit. L'ente di certificazione guiderà il processo, che include generalmente un audit di transizione per verificare la conformità ai nuovi requisiti.

Quanto tempo richiede la certificazione ISO 27701?

Le tempistiche variano in base alla dimensione dell'organizzazione, alla complessità dei dati e all'eventuale presenza di un sistema di gestione già implementato. Le organizzazioni con una governance privacy matura possono completare la transizione in un singolo ciclo di audit, mentre quelle senza certificazioni ISO potrebbero necessitare di diversi mesi per implementare e rendere operative le misure richieste. Un gap assessment iniziale è il modo più affidabile per stabilire una tempistica realistica.