CIRCOLARE TECNICA

Prot. DC2026SPM089 **Milano**, 17-06-2026

A tutti gli Organismi di certificazione accreditati/accreditandi
Alle Associazioni degli Organismi di valutazione della conformità
A tutti gli Ispettori/Esperti del Dipartimento DC

Loro sedi

OGGETTO: Circolare tecnica DC N. 23/2026 - Disposizioni in merito all'accreditamento UNI CEI EN ISO/IEC 17021-1 degli Organismi di Certificazione a fronte della norma ISO/IEC 27701

Premessa

Il presente documento fornisce disposizioni e indirizzi per l'accreditamento degli Organismi di certificazione (in seguito OdC) operanti in conformità alla UNI CEI EN ISO/IEC 17021-1 per la certificazione Privacy Information Management Systems (PIMS) a fronte della norma UNI CEI EN ISO/IEC 27701:2025 (d'ora in avanti abbreviata in ISO/IEC 27701).

Si segnala che, anche se molti argomenti trattati dalla Norma hanno riscontro in specifici requisiti di legge nazionali, sia in Italia, sia in altri Paesi dell'Unione Europea, disciplinati dal GDPR e dalle precedenti Leggi nazionali, la Norma, basandosi sulla ISO 17021-1, non è da considerarsi, allo stato, aderente ai meccanismi di certificazione, definiti dall'Art. 42 del GDPR.

La norma ISO/IEC 27701 costituisce uno standard internazionale certificabile per la gestione della protezione dei dati personali e della privacy, applicabile alle organizzazioni che operano quali PII Controller e/o PII Processor. A differenza della precedente edizione, che era strutturata come estensione della ISO/IEC 27001, la nuova versione della norma consente la certificazione del sistema di gestione della privacy anche come schema autonomo.
Per ottenere l'Accreditamento a fronte della Norma citata, gli OdC devono soddisfare non solo i requisiti della norma UNI CEI EN ISO/IEC 17021-1, ma anche quelli della norma UNI CEI EN ISO/IEC 27706:2025 (d'ora in avanti abbreviata in ISO/IEC 27706), quale norma di Livello 4 secondo il documento EA 1/06.

Le caratteristiche del servizio di valutazione della conformità

La certificazione PIMS ha lo scopo di valutare l'adeguatezza e l'efficace implementazione di un sistema di gestione della privacy basato:

- sull’analisi del contesto e delle parti interessate;
- sulla valutazione e trattamento del rischio privacy;
- sull’adozione dei controlli di cui all’Annex A della ISO/IEC 27701.

La norma, basata anch’essa sulla struttura HS e sul ciclo PDCA, prevede come step iniziale un’analisi accurata dell’ambito di trattamento che si vuole certificare, prendendo in considerazione il contesto, all’interno del quale devono essere individuate le esigenze delle parti interessate, interne ed esterne, rilevanti e in grado di influenzare la capacità del PIMS di raggiungere i risultati desiderati. Una volta definito il trattamento di dati personali da sottoporre a certificazione, viene richiesto che gli effetti dello stesso sui PII principals e, più in generale, sui diritti e sulle libertà fondamentali delle persone fisiche, siano oggetto di un processo strutturato di valutazione del rischio privacy, idoneo a evidenziare come tutte le fasi del trattamento — dalla raccolta alla conservazione, dall’utilizzo alla comunicazione, fino alla cancellazione o anonimizzazione dei dati — siano governate in modo tale da garantire la liceità, la correttezza, la trasparenza e la sicurezza del trattamento. Ne deriva che, oltre agli aspetti organizzativi e tecnici connessi al trattamento dei dati personali, venga posta particolare attenzione all’approccio di governance adottato dall’organizzazione in materia di protezione dei dati, orientato ai principi di responsabilizzazione (accountability), minimizzazione, proporzionalità e tutela dei diritti dei PII principals. In tale contesto, gli OdC sono chiamati a valutare non solo l’adeguatezza delle misure tecniche e organizzative implementate, ma anche la coerenza e l’efficacia del sistema di governo dei trattamenti, in relazione alle finalità perseguite, ai rischi individuati e alle esigenze delle parti interessate. Questa impostazione intende valorizzare le scelte consapevoli e responsabili delle organizzazioni nell’ambito della gestione della privacy, promuovendo un approccio sostenibile e sistematico alla protezione dei dati personali, in grado di rafforzare la fiducia delle parti interessate e dei soggetti cui i dati si riferiscono. Infatti, una volta definiti il contesto dell’organizzazione e le esigenze delle parti interessate, l’organizzazione, attraverso il proprio assetto organizzativo e il coinvolgimento della direzione, è chiamata a definire una politica per la protezione dei dati personali, a stabilire obiettivi misurabili, ad attribuire ruoli e responsabilità, a pianificare e attuare le attività di valutazione e trattamento dei rischi privacy, nonché a predisporre adeguati meccanismi di controllo, monitoraggio e riesame dell’efficacia del Privacy Information Management System, fino al completamento del ciclo Plan–Do–Check–Act (PDCA).

Regole di Transizione

Si segnala che sono soggetti a transizione tutti gli OdC:

- accreditati per la ISO/IEC 27701:2019 in scopo fisso;
- che attualmente referenziano la ISO/IEC 27701:2019 nello scopo flessibile della famiglia delle norme ISO 27000. Al completamento della transizione, questi OdC saranno accreditati per la ISO/IEC 27701:2025 con scopo fisso.

Transizione dell’Accreditamento	A partire dal 1° luglio 2026 ACCREDIA non accetterà nessuna nuova domanda di accreditamento nello schema MS (PIMS) che faccia riferimento alla norma di certificazione

	ISO/IEC 27701:2019 ed emetterà nuovi accreditamenti nello schema MS (PIMS) solo a fronte della norma di certificazione ISO/IEC 27701:2025. ACCREDIA verificherà l'adeguamento del processo di certificazione alla nuova norma (verifica di transizione) attraverso un esame documentale off-site della durata di 1 giorno/uomo. Per la conduzione dell'esame documentale si veda l'Allegato "Self Assessment Piano di Transizione". Il termine ultimo per il completamento della transizione dell'accreditamento è il 31 ottobre 2027. Dal 1° novembre 2027 tutti gli accreditamenti non transitati alla nuova norma saranno revocati.
Transizione delle certificazioni	Considerato che le organizzazioni certificate ISO/IEC 27701 risultano già certificate ISO/IEC 27001:2022 e che la revisione della norma ISO/IEC 27701:2025 non introduce modifiche sostanziali ai controlli applicabili ai PII controller e ai PII processor, non è richiesto un audit di transizione dedicato. Si richiede tuttavia agli OdC di effettuare per ogni cliente una gap analysis, al fine di ottenere le informazioni necessarie, a fronte delle quali adeguare il contratto di certificazione. Sarà possibile erogare le giornate di audit complementari, se necessarie, alla prima verifica utile presso l'azienda o con un audit straordinario. A esito positivo di tale verifica l'OdC potrà rilasciare il certificato aggiornato. Tutte le certificazioni emesse sotto accreditamento a fronte della ISO/IEC 27701:2019 dovranno essere transitate al nuovo standard entro il 31 marzo 2028. Dal 1 aprile 2028 tutte le certificazioni non transitate alla nuova norma dovranno essere revocate.

Regole di Certificazione

Si applicano le prescrizioni della norma UNI CEI EN ISO/IEC 17021-1 integrata dalla ISO/IEC 27706.

Calcolo delle durate dei tempi di audit	Si applicano i requisiti applicabili della UNI CEI EN ISO/IEC 17021-1 integrati dalla ISO/IEC 27706.
Durata del certificato e frequenze di audit	Si applicano i requisiti applicabili della UNI CEI EN ISO/IEC 17021-1 integrati dalla ISO/IEC 27706.
Criteri di competenza del personale addetto alla valutazione della conformità	Si applicano i requisiti applicabili della UNI CEI EN ISO/IEC 17021-1 integrati dalla ISO/IEC 27706.
Documenti Global ACI applicabili	Trovano applicazione tutti i documenti Global ACI (già IAF) relativi ai sistemi di gestione.

Banca dati ACCREDIA delle certificazioni rilasciate

Come noto, gli OdC sono tenuti a trasmettere ad ACCREDIA-DC tramite il servizio web – SIAC i dati relativi ai soggetti in possesso di certificazioni da essi rilasciate, secondo le procedure definite da ACCREDIA-DC e i relativi Regolamenti (RG01 §1.10.7).

Regole di Accreditamento

A	OdC già accreditato per gli schemi UNI CEI EN ISO/IEC 17021-1:2015 e ISO/IEC 27001	• Esame Documentale di 0,5 g/u; • 1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente.
B	OdC già accreditato per gli schemi UNI CEI EN ISO/IEC 17021-1:2015 ma non ISO/IEC 27001	• Esame Documentale di 0,5 g/u; • Verifica in sede presso la sede dell'OdC della durata di 1 g/u; • 1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente.
C	OdC non ancora accreditato UNI CEI EN ISO/IEC 17021-1:2015 ma accreditato per altri schemi di accreditamento (Livello 3)	• Esame documentale di 1 g/u; • Verifica ispettiva presso la sede dell'OdC della durata di 2 g/u; • 1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente.
D	OdC non accreditato	• Esame documentale di 1 g/u da svolgersi, se possibile, in parte in modalità sincrona da remoto; • Verifica ispettiva presso la sede dell'OdC della durata di 4 g/u; • 1 Verifica in accompagnamento di durata adeguata.

Mantenimento dell'Accreditamento

Si ricorda che ACCREDIA-DC, in ogni caso, deve condurre annualmente una verifica presso la sede degli OdC per valutarne la conformità alla UNI CEI EN ISO/IEC 17021-1.
Fatta eccezione per situazioni particolari (es: trend di certificati rilasciati, gestione reclami e segnalazioni, modifiche intervenute sullo schema di certificazione, cambiamenti nella struttura dell'OdC o altre situazioni similari), tenuto conto della complessità dello schema, ACCREDIA effettuerà le seguenti verifiche nel ciclo di accreditamento:

N. Certificati rilasciati	
0÷50	2 Verifiche in sede 1 Verifica in accompagnamento
>50	3 Verifiche in sede 1 Verifiche in accompagnamento

Documentazione da presentare ad ACCREDIA-DC per l'esame documentale

Oltre a quanto elencato nella domanda di accreditamento DA-01 si richiede l'invio di:

a. Liste di riscontro, linea guida, istruzioni predisposte dall'OdC per il GVI;
b. Criteri di qualifica e curricula del personale addetto al riesame del contratto, degli auditor (compresi eventuali esperti tecnici per l'area di business del cliente) e dei technical reviewer/decision maker con le relative schede di qualifica;
c. Procedure applicabili al processo commerciale per la definizione dei tempi di audit, nonché le procedure per la gestione della pratica di certificazione.

Cogliamo l'occasione per porgere cordiali saluti.

Dott.ssa Mariagrazia Lanzanova

Vice-Direttore Dipartimento
Certificazione e Ispezione

Firmato digitalmente da: MARIAGRAZIA LANZANOVA
Data: 17/06/2026 16:31:43