TECHNICAL CIRCULAR

Ref. DC2026SPM116 **Milan**, 15-09-2026

To all accredited/accreditation-seeking Certification Bodies
To the Associations of Conformity Assessment Bodies
To all Assessors/Experts of the DC Department

Their offices

SUBJECT: Technical Circular DC No. 33/2026 - CORRIGENDUM to Technical Circular DC No. 23/2026 - Provisions concerning UNI CEI EN ISO/IEC 17021-1 accreditation of Certification Bodies against the ISO/IEC 27701 standard

This Technical Circular cancel and replaces the previous Technical Circular DC No. 23/2026 DC2026SPM089 of 17/06/2026. The changes made are indicated by a side bar.

Foreword

This document provides provisions and guidance for the accreditation of Certification Bodies (hereinafter CBs) operating in accordance with UNI CEI EN ISO/IEC 17021-1 for the certification of a privacy information management system (PIMS) against the UNI CEI EN ISO/IEC 27701:2025 standard (hereinafter abbreviated to ISO/IEC 27701).

It should be noted that, although many of the topics covered by the standard correspond to the GDPR and to specific national legal requirements in Italy and other European Union countries, the standard, being based on ISO 17021-1, is not to be regarded as a certification mechanism within the meaning of Article 42 of the GDPR.

ISO/IEC 27701 is a certifiable international standard for a privacy information management system, applicable to organisations acting as PII controllers or PII processors, or both, in the processing of personal data. Unlike the previous edition, which was structured as an extension of ISO/IEC 27001, the new version of the standard allows the privacy information management system to be certified as a standalone management system.
In order to obtain accreditation against the above-mentioned standard, CBs must satisfy not only the requirements of UNI CEI EN ISO/IEC 17021-1, but also those of UNI CEI EN ISO/IEC 27706:2025 (hereinafter abbreviated to ISO/IEC 27706), as a Level 4 standard in accordance with document EA 1/06.

Characteristics of the conformity assessment service

The purpose of PIMS certification is to assess the adequacy and effective implementation of a privacy information management system based on:

- analysis of the context and of interested parties;
- privacy risk assessment and treatment;
- the adoption of the controls necessary to implement the privacy risk treatment options.

The standard, also based on the HS structure and the PDCA cycle, requires as an initial step a thorough analysis of the scope of processing to be certified, taking into account the context, within which the relevant needs of internal and external interested parties, capable of influencing the PIMS's ability to achieve its intended outcomes, must be identified. Once the processing operation(s) of personal data to be submitted for certification have been defined, it is required that the effects thereof on data subjects (PII principals) and, more generally, on the fundamental rights and freedoms of natural persons, be subject to a structured privacy information risk assessment process, capable of demonstrating that all stages of processing — from collection to storage, from use to disclosure, through to erasure or anonymisation of the data — are governed in such a way as to ensure the lawfulness, fairness, transparency and security of the processing. It follows that, in addition to the organisational and technical aspects connected with the processing of personal data, particular attention must be paid to the data protection governance approach adopted by the organisation, oriented towards the principles of accountability, minimisation, proportionality and protection of data subjects' rights. In this context, CBs are required to assess not only the adequacy of the technical and organisational measures implemented, but also the consistency and effectiveness of the processing governance system, in relation to the purposes pursued, the risks identified and the needs of interested parties. This approach is intended to promote informed and responsible choices by organisations in the field of privacy management, fostering a sustainable and systematic approach to the protection of personal data, capable of strengthening the trust of interested parties and of the individuals to whom the data relate. Indeed, once the context and the needs of interested parties have been defined, the organisation, through its own organisational structure and the involvement of top management, is required to define a personal data protection policy, to establish measurable objectives, to assign roles and responsibilities, to plan and carry out privacy risk assessment and treatment activities, as well as to put in place the controls necessary to implement the privacy risk treatment options and the activities for monitoring and reviewing the effectiveness of the Privacy Information Management System, through to completion of the Plan–Do–Check–Act (PDCA) cycle.

With regard to the controls set out in Annex A of ISO/IEC 27701, attention is drawn to the following:

- Table A.1 sets out controls specific to PII controllers;
- Table A.2 sets out controls specific to PII processors;
- Table A.3 sets out certain information security controls for PII controllers and processors;

- the controls in Annex A, and in particular in Annex A.3, are not to be regarded as exhaustive. Depending on the outcomes of the risk assessment, the applicable legal, regulatory and contractual requirements, and the information security programme adopted, additional controls may be necessary, for example relating to asset inventory, business continuity, physical security, etc.;
- the Statement of Applicability must include all controls identified as necessary pursuant to clause 6.1.3 of ISO/IEC 27701, even where derived from sources other than Annex A. It must set out the necessary controls, the justification for their inclusion, their implementation status, and the justification for the exclusion of any Annex A controls that are not applicable.

Transition rules

It should be noted that all CBs are subject to transition where they are:

- accredited for ISO/IEC 27701:2019 under fixed scope;
- currently reference ISO/IEC 27701:2019 under the flexible scope of the ISO/IEC 27000 family of standards. Upon completion of the transition, these CBs will be accredited for ISO/IEC 27701:2025 under fixed scope.

Transition of Accreditation	As of 1 July 2026, ACCREDIA will no longer accept any new application for accreditation under the MS (PIMS) scheme that refers to the ISO/IEC 27701:2019 certification standard, and will issue new accreditations under the MS (PIMS) scheme only against the ISO/IEC 27701:2025 certification standard. ACCREDIA will verify the adaptation of the certification process to the new standard (transition audit) by means of an off-site document review lasting 1 man-day. For the conduct of the document review, see the Annex "Self-Assessment Transition Plan". The deadline for completing the accreditation transition is 31 October 2027. As of 1 November 2027, all accreditations that have not transitioned to the new standard will be withdrawn.
Transition of certifications	Given that organisations certified to ISO/IEC 27701 are already certified to ISO/IEC 27001:2022, and that the revision of ISO/IEC 27701:2025 does not introduce substantial changes to the controls applicable to PII controllers and PII processors, a dedicated transition audit is not required. However, CBs are required to carry out a gap analysis for each client in order to obtain the necessary information, on the basis of which the certification contract must be updated. Any additional audit days, if necessary, may be delivered at the next useful audit at the organisation's premises or by means of a special audit. Upon a positive outcome of this audit, the CB may issue the updated certificate. All certifications issued under accreditation against ISO/IEC 27701:2019 must transition to the new standard by 31 March 2028. As of 1 April 2028, all certifications that have not transitioned to the new standard must be withdrawn.

Certification Rules

The requirements of UNI CEI EN ISO/IEC 17021-1, supplemented by ISO/IEC 27706, apply.

Calculation of audit time durations	The applicable requirements of UNI CEI EN ISO/IEC 17021-1, as supplemented by ISO/IEC 27706, apply
Certificate validity and audit frequencies	The applicable requirements of UNI CEI EN ISO/IEC 17021-1, as supplemented by ISO/IEC 27706, apply.
Competence criteria for personnel involved in conformity assessment	The applicable requirements of UNI CEI EN ISO/IEC 17021-1, as supplemented by ISO/IEC 27706, apply.
Applicable Global ACI documents	All Global ACI (formerly IAF) documents relating to management systems apply.

ACCREDIA database of certifications issued

As is well known, CBs are required to transmit to ACCREDIA-DC, via the SIAC web service, the data relating to the parties holding certifications issued by them, in accordance with the procedures defined by ACCREDIA-DC and the relevant Regulations (RG01 §1.10.7).

Accreditation Rules

A	CB already accredited for the UNI CEI EN ISO/IEC 17021-1:2015 and ISO/IEC 27001 schemes	• Document Review of 0.5 man-days; • 1 witness assessment of a duration commensurate with the client's organisational size.
B	CB already accredited for the UNI CEI EN ISO/IEC 17021-1:2015 scheme but not for ISO/IEC 27001	• Document Review of 0.5 man-days; • Office assessment at the CB's premises lasting 1 man-day. • 1 witness assessment of a duration commensurate with the client's organisational size.
C	CB not yet accredited to UNI CEI EN ISO/IEC 17021-1:2015 but accredited for other accreditation schemes (Level 3)	• Document review of 1 man-day; • Assessment at the CB's offices lasting 2 man-days; • 1 witness assessment of a duration commensurate with the client's organisational size.
D	Non-accredited CB	• Document review of 1 man-day, to be carried out, where possible, partly in synchronous remote mode; • Assessment at the CB's offices lasting 4 man-days; • 1 witness assessment of an appropriate duration.
Maintenance of Accreditation	It should be noted that ACCREDIA-DC must, in any case, conduct an annual assessment at the offices of CBs to assess their conformity with UNI CEI EN ISO/IEC 17021-1. With the exception of particular situations (e.g. trends in certificates issued, management of complaints and reports, changes to the certification scheme, changes in the CB's structure,	

	or other similar situations), taking into account the complexity of the scheme, ACCREDIA will carry out the following assessments during the accreditation cycle: No. of certificates issued 0÷50 — 2 Office assessments, 1 Witness Assessment >50 — 3 Office assessments, 1 Witness Assessment

Documentation to be submitted to ACCREDIA-DC for the document review

In addition to what is listed in the DA-01 accreditation application, the following must also be submitted:

a. Checklists, guidelines and instructions prepared by the CB for the assessment team;

b. Qualification criteria and CVs of the personnel responsible for contract review, of the auditors (including any technical experts for the client's business area), and of the technical reviewers/decision makers, together with the relevant qualification records;

c. Procedures applicable to the commercial process for determining audit durations, as well as the procedures for managing the certification file.

Mariagrazia Lanzanova

Vice-Director

Certification and Inspection Department

Firmato digitalmente da: MARIAGRAZIA LANZANOVA
Data: 15/09/2026 15:20:16