SmartSuite

Framework / Privacy / ISO 27000 Series

ISO/IEC 27701:2025 Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

ISO/IEC 27701:2025 specifies requirements for a stand-alone privacy information management system (PIMS) for PII controllers and processors, replacing the 2019 edition.



What it is

ISO/IEC 27701:2025 is the international standard that specifies requirements for establishing, implementing, maintaining and continually improving a privacy information management system (PIMS), for organizations acting as PII controllers or PII processors. ISO and IEC published this second edition on October 14, 2025, prepared by ISO/IEC JTC 1/SC 27 with CEN/CLC/JTC 13; it cancels and replaces ISO/IEC 27701:2019, which ISO withdrew. The 2019 edition extended ISO/IEC 27001 and 27002, while the 2025 edition has been redrafted as a stand-alone management system standard.

Any organization that holds responsibility and accountability for processing personally identifiable information (PII) can use it, whatever its type or size (Clause 1). Requirements sit in Clauses 4 to 10, and two normative annexes follow: Annex A, the PIMS reference control objectives and controls for PII controllers and PII processors, and Annex B, the implementation guidance. Annexes C to F, which are informative, map it to ISO/IEC 29100, the GDPR, ISO/IEC 27018 and 29151, and the 2019 edition.

At a glance

PUBLISHER International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)	TYPE Standard	VERSION ISO/IEC 27701:2025 (second edition); replaces 2019 edition
EFFECTIVE October 14, 2025	DOMAIN Privacy	FAMILY ISO 27000 Series
REGION International	ADOPTION MODEL Certification	IMPLEMENTATION COMPLEXITY High

Source: iso.org/standard/85819.html

Why it matters

- **Evidence of how PII is handled** By meeting the requirements an organization can generate evidence of how it processes PII, which can support agreements with business partners (Introduction 0.1).
- **Independent verification** The use of the document can provide independent verification of that evidence, and interested parties can call for independently audited conformity (Introduction 0.1; Clause 4.2, Note 6).
- **Roles that are stated** The organization determines whether it acts as a PII controller, including a joint PII controller, or as a PII processor, and keeps separate controls where it is both (Clause 4.1).
- **One system with other standards** It applies ISO's harmonized management system framework, so a PIMS can be aligned or integrated with other standards, in particular the ISMS in ISO/IEC 27001 (Introduction 0.2).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ISO 27701

Roles and Processing Inventory

Use Privacy Management to keep data inventories that show, for each processing activity, whether you act as a PII controller, joint controller or PII processor (Clause 4.1).

Interested Parties and Requirements

Record interested parties, including PII principals and supervisory authorities, and the requirements you address through the PIMS (Clause 4.2).

Privacy Risk Assessment and Treatment

Run privacy assessments and track privacy risks, treatment plans and approvals with evidence attached (Clauses 6.1.2, 6.1.3, 8.2 and 8.3).

Controls and Statement of Applicability

Use Compliance Management to hold the Annex A controls with applicability, justification and implementation status (Clause 3.25; Annex A).

Processor and Sub-contractor Oversight

Use Third Party Risk Management to assess and monitor the processors and sub-contractors you rely on, with contract terms and review evidence (Clause 4.2).

Internal Audit and Management Review

Use Internal Audit Management to plan audits and track nonconformities and corrective actions, and record management review inputs and results (Clauses 9.2, 9.3 and 10.2).

Common framework mappings

GDPR | ISO 27001:2022 | ISO 27002:2022 | ISO 27017 | ISO 27018 | ISO 29100 | NIST Privacy Framework v1.0 | SOC 2

Official resources

ISO/IEC 27701:2025 Standard

ISO/IEC 27701:2025, the second edition (October 14, 2025), on the ISO catalog.

iso.org/standard/85819.html

ISO/IEC 27701 Implementation Guidance

Provides guidance for implementing privacy controls in compliance with ISO/IEC 27701.

iso.org/isoiec-27701-privacy-information-management.html

Frequently asked questions

What changed between ISO/IEC 27701:2019 and ISO/IEC 27701:2025?

The Foreword gives one main change: the document has been redrafted as a stand-alone management system standard, where the 2019 edition extended ISO/IEC 27001 and 27002. The 2025 edition has requirements in Clauses 4 to 10, normative Annexes A and B for controls and guidance, and Annex F with the correspondence to the 2019 edition. ISO withdrew the 2019 edition.

Do I need ISO/IEC 27001 to use ISO/IEC 27701:2025?

The document is a stand-alone management system standard, and ISO's catalog page says it can be used alone. Introduction 0.2 states that it enables an organization to align or integrate its PIMS with other management system standards, in particular ISO/IEC 27001, so an existing ISMS can share structure and processes.

Who is ISO/IEC 27701:2025 for?

It is intended for PII controllers and PII processors holding responsibility and accountability for PII processing (Clause 1). Clause 4.1 requires the organization to determine its role, including as a joint PII controller, and where it acts in both roles, each role is the subject of a separate set of controls.

How does certification and the transition from the 2019 edition work?

Accredited certification bodies audit PIMS against ISO/IEC 27701 using ISO/IEC 27706:2025, which replaces ISO/IEC TS 27006-2:2021. The Singapore Accreditation Council set October 31, 2027 for its certification bodies to transition and October 31, 2028 for moving all clients to the 2025 edition. Your own deadline depends on your accreditation body and certification body.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What are Annexes A and B in ISO/IEC 27701:2025?

Annex A (normative) lists the PIMS reference control objectives and controls for PII controllers and PII processors. Annex B (normative) gives implementation guidance for both roles. Annexes C to E map the standard to ISO/IEC 29100, the GDPR, and ISO/IEC 27018 and 29151, and the mappings can be read against local legal requirements (Introduction 0.1).

License included / downloadable: No ISO/IEC 27701:2025 is a paid standard sold by ISO and national standards bodies, and the text is not included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/iso-iec-27701-privacy-information-management-system-pims

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.