

ISO/IEC 27701:2019 (PIMS)

ISO/IEC 27701 extends ISO/IEC 27001 to help organizations manage privacy and protect personally identifiable information.



What it is

ISO/IEC 27701 is an international privacy information management standard that helps organizations establish, implement, maintain, and continually improve a Privacy Information Management System (PIMS). Its primary purpose is to extend the requirements of ISO/IEC 27001 and ISO/IEC 27002 to address privacy and data protection, supporting compliance with data privacy regulations and risk management objectives.

Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27701 serves organizations of all sizes and sectors handling personally identifiable information (PII). The framework covers areas including privacy governance, data protection controls, accountability, and regulatory compliance alignment, making it relevant to entities subject to global data privacy laws such as the GDPR.

At a glance

PUBLISHER International Organization for Standardization (ISO)	TYPE Standard	VERSION 2019
EFFECTIVE August 2019	DOMAIN Privacy	FAMILY ISO 27000 Series
REGION International	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: <https://www.iso.org/standard/71670.html>

Why it matters

- **Strengthen privacy governance** Establish clear structures and defined responsibilities around privacy management to support organizational accountability and oversight.
- **Enhance regulatory alignment** Align privacy practices with global regulations, such as GDPR, to demonstrate compliance and facilitate cross-border data activities.
- **Support risk-based data protection** Enable organizations to assess and mitigate privacy risks, tailoring controls to match business needs and risk profiles.
- **Increase audit and certification readiness** Provide a standardized framework for evidencing compliance and preparing for external audits or privacy-specific certifications.

How SmartSuite supports ISO 27701

PIMS Extension to Your ISMS

Run privacy governance as an extension of ISO 27001 with shared structure and cadence.

Processing Inventory and Accountability

Maintain records of processing, roles, responsibilities, and purpose documentation.

DPIAs and Privacy Risk Management

Track privacy risk assessments, approvals, mitigation tasks, and evidence.

DSAR Workflows and Audit Trail

Manage rights requests end-to-end with deadlines, responses, and documentation.

Vendor, Processor, and Subprocessor Controls

Oversee vendors with contract controls, reviews, and monitoring evidence.

Audit-Ready Privacy Reporting

Report privacy control coverage, open risks, and readiness across the program.

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 Standard

Defines requirements for establishing a Privacy Information Management System, extending ISO/IEC 27001.
iso.org/standard/71670.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 is ISO/IEC 27701 used for?

ISO/IEC 27701 is used to establish and maintain a Privacy Information Management System (PIMS), extending the ISO/IEC 27001 Information Security Management System to include privacy and personal data protection controls. Organizations adopt this standard to systematically manage risks associated with personally identifiable information (PII) and demonstrate alignment with global privacy regulations such as GDPR.

Is ISO/IEC 27701 certifiable or mandatory?

ISO/IEC 27701 is a certifiable standard, which means organizations can achieve formal certification through accredited third-party audits. While it is not legally mandatory, it is widely recognized and can support legal and regulatory compliance efforts by providing evidence of structured privacy management practices.

What types of organizations should implement ISO/IEC 27701?

ISO/IEC 27701 is applicable to any organization—regardless of size, sector, or geography—that processes PII either as a controller or processor. It is particularly relevant for organizations subject to privacy regulations or those seeking to enhance their privacy posture and demonstrate accountability.

What are the key concepts and documentation required by ISO/IEC 27701?

Key concepts include privacy governance, roles and responsibilities (controller and processor), risk assessments, Data Protection Impact Assessments (DPIAs), and records of processing activities. Required documentation typically includes a Statement of Applicability (SoA) for privacy controls, privacy policies, and procedures for vendor management and incident response.

How do organizations implement ISO/IEC 27701 in practice?

Implementation involves integrating ISO/IEC 27701 privacy controls with existing ISO/IEC 27001 security controls, assigning privacy roles, conducting privacy risk assessments, and maintaining required records. Ongoing activities include regular reviews, privacy training, monitoring compliance obligations, and responding to privacy-related incidents.

What is the relationship between ISO/IEC 27701 and other frameworks like ISO/IEC 27001 or GDPR?

ISO/IEC 27701 builds on ISO/IEC 27001 by layering privacy-specific requirements on top of existing information security processes. It provides a structured approach for aligning with privacy laws like GDPR by defining roles, obligations, and accountability measures, and by supporting the mapping of privacy requirements to established security controls.

What ongoing compliance activities are required under ISO/IEC 27701?

Ongoing compliance with ISO/IEC 27701 requires maintaining up-to-date risk assessments, continual monitoring of privacy controls, regular audits, employee training, and effective incident response processes. Organizations must also document data processing activities and review privacy obligations in line with regulatory changes.

How would SmartSuite support ISO/IEC 27701 (Privacy Information Management System)?

SmartSuite enables organizations to manage ISO/IEC 27701 compliance by providing tools for tracking privacy-related risks, managing and monitoring privacy controls, and collecting evidence for audits. The platform supports maintaining documentation, compliance tracking, remediation workflows, and dashboard reporting to demonstrate ongoing privacy management and audit readiness.

License included / downloadable: No ISO/IEC 27701 requires purchase through the ISO standards catalog. License not included with platform

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