Privacy Information Management with ISO/IEC 27701

Your implementation guide

Contents

What is ISO/IEC 27701?

To earn and hold the digital trust of customers and other stakeholders, both personally identifiable information (PII) processors and PII controllers must have robust data processes and controls in place. Furthermore, increasing privacy regulation around the world is driving the need for demonstrating effective and transparent management of PII.

Standards are the surest way to demonstrate accountability for managing PII, instil trust and build strong business relationships. Plus, they form the foundationon which to build compliance with regulatory requirements.

The standard to aim for is ISO/IEC 27701, the international standard for a Privacy Information Management System (PIMS) and a privacy extension to ISO/IEC 27001 Information Security Management and ISO/IEC 27002 Security Controls.

What kind of organizations can benefit from a Privacy Information Management System?

Organizations of all industries and sizes—whether public, private, government or not-for-profit—around the world use ISO/IEC 27701 to prove they take protecting personal information seriously. Specific organizational roles includes:

- PII controllers (including those who are joint PII controllers)
- PII processors

Benefits of ISO/IEC 27701

- Builds trust in managing PII
- Supports compliance with privacy regulations
- Reduces complexity by integrating with ISO/IEC 27001
- Facilitates effective business relationships
- Clarifies roles and responsibilities

The key requirements of ISO/IEC 27701

Organizations must meet these eight clauses in order to be certified.

Clause 1: Scope

Sets out the requirements for the management system and its intended application.

ISO/IEC 27701 is aimed at providing requirements and guidance to establish, implement, maintain and improve a privacy information management system for both PII controllers and PII processors who hold responsibility and accountability for processing PII.

Clause 2: Normative references

Normative references are documents referred to throughout a standard. For ISO/IEC 27701 these include:

- ISO/IEC 27000 Information security management systems – overview and vocabulary
- ISO/IEC 27001 Information security management systems – requirements
- ISO/IEC 27002 Code of practice for information security controls
- ISO/IEC 29100 Privacy framework

Clause 3: Terms and definitions

This section provides a couple of additional definitions for important terms used throughout the standard that are not included in ISO/IEC 27000 and ISO/IEC 29100

Clause 4: General

Clause 4 sets the scene for ISO/IEC 27701, with an overview of the document's structure and a high-level indication of the location of PIMS specific requirements in relation to both ISO/IEC 27001 and ISO/IEC 27002

Clause 5: PIMS specific requirements related to ISO/IEC 27001

This clause is all about extending information security requirements from ISO/IEC 27001 to incorporate the protection of privacy.

As part of the context of the organization, you need to determine your role as a processor and/or controller and consider the impact of internal and external factors such as privacy specific regulations and contractual requirements. Depending on your role, relevant controls from Annexes A and/or B need to be implemented and applied to your existing statement of applicability.

You must also consider interested parties associated with processing PII, the scope of your PIMS and how you'll effectively implement, maintain and continually improve the system.

Requirements for leadership, planning, support, operation, performance evaluation and improvement from ISO/IEC 27001 must be considered and extended as appropriate to ensure the protection of privacy. In particular, risks to information and processing of PII must now be assessed and treated appropriately.

Clause 6: PIMS specific guidance related to ISO/IEC 27002

This clause is all about extending information security guidance from ISO/IEC 27002 to incorporate the protection of privacy.

For example, organizations need to consider the additional implementation guidance around information security policies to incorporate relevant privacy statements, based on compliance, contractual and stakeholder requirements.

Clearer guidance is provided on roles and responsibilities in relation to PII processing. This includes awareness of incident reporting and the consequences of a privacy breach.

Guidance to ensure consideration of PII within your information classification is provided. You must understand the PII your organization processes, where it is stored and the systems it flows through. People must also be aware of what PII is and how to recognize it.

More detailed implementation guidance is included on incident management, removable media, user access on systems and services that process PII, cryptographic protection, re-assigning storage space that previously stored PII, back-up and recovery of PII, event log reviews, information transfer policies and confidentiality agreements.

Plus, guidance in this clause encourages you to consider PII up front before data transmission on public networks, and as part of system development and design. Importantly, supplier relationships, expectations and responsibilities need addressing.

Clause 7: Additional guidance for PII controllers

This clause covers PIMS specific implementation guidance for PII controllers. It relates to controls listed in Annex A.

For example, you need to identify the specific purposes for the PII you process and have a legal basis for processing it to comply with relevant laws. Updates should be made if the purpose for processing PII changes or extends.

Guidance also outlines considerations of special category data and consent requirements, privacy impact assessment requirements to minimize risk to PII principals, contracts with PII processors and clear roles and responsibilities with any joint controllers.

You should make it clear to individuals whose PII you process why and how you process it, with a contact point for any requests. Detailed guidance is included on consent, withdrawals and PII access, correction or erasure. Third party obligations, handling requests and automated decision-making guidance is also provided.

Finally, privacy by design for processes and systems should consider minimum requirements for collection and processing, the accuracy and quality of PII, limitations on the amount collected based on the purpose of processing and end of processing requirements.

Importantly, PII sharing, transfer and disclosure guidance is outlined to help you transfer between jurisdictions with supporting records.

Clause 8: Additional guidance for PII processors

This clause covers PIMS specific implementation guidance for PII processors. It relates to controls listed in Annex B.

For example, customer contracts should address your organization's role as a PII processor to assist with customer obligations, including those of PII principals. Prior consent must be made to use PII data for marketing and advertising purposes.

Guidance is outlined to identify and maintain the necessary records to help demonstrate compliance with agreed PII processing you conduct.

The standard also includes detailed guidance on a range of privacy-specific activities, such as responding to individual disclosure requests, managing temporary files created during processing, returning, transferring or disposing of PII securely, and applying appropriate transmission controls.

Finally, PII sharing, transfer and disclosure guidance is detailed to address jurisdictional transfers, third-party and sub-contractor requirements and management of legally binding PII disclosures.

Annexes

A number of Annexes are also included in ISO/IEC 27701. Annexes A and B are for controllers and processors respectively, whilst annexes C – F provide additional knowledge that can support with setting up and operating an effective PIMS.

Annex A

A list of controls for PII controllers.

Not all controls will be required, however a justification for excluding any control is required in the statement of applicability.

Annex B

A list of controls for PII processors.

Not all controls will be required, however a justification for excluding any control is required in the statement of applicability.

Annex C

Mapping of controls for PII controllers to the ISO/IEC 29100 privacy principals.

This shows an indication of how compliance to requirements and controls of ISO/IEC 27701 relate to the privacy principals in ISO/IEC 29100.

Annex D

Mapping of ISO/IEC 27701 clauses to GDPR articles 5 to 49 (except 43).

This shows how compliance to requirements and controls of ISO/IEC 27701 can be relevant to fulfilling obligations of GDPR.

Annex E

Mapping of ISO/IEC 27701 clauses to:

- ISO/IEC 27018 requirements for PII processors in public clouds
- ISO/IEC 29151 for additional controls and guidance for PII controllers.

Annex F

Details how to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002.

It clearly maps the extension of information security terms to incorporate privacy and includes some examples for application.

Train with BSI

To create digital trust for your customers and your supply chain, you must ensure that personal data and commercially sensitive information is secured from business risk and vulnerabilities.

BSI's range of digital trust and information security training courses and professional qualifications can accelerate your journey to digital trust, by providing the knowledge and skills you need to build resilience in your organization and maximize performance.

You can take it further with additional privacy information management training courses to help you maximize ISO/IEC 27701 for your organization and go deeper with the standard.

Our courses are delivered via a high-impact, accelerated learning approach, proven to enhance retention and skill application.

Learn in a way that works for you:

Classroom-based training
Convenient location and dates, delegates from multiple organizations.

Virtual instructor led training
Available as both classroom and in-house options.

On-demand eLearning
Self-paced, online, available 24/7 – for complete flexibility.

In-house training
Client's chosen location and dates, adaptable to organizational requirements.

BSI Connect

Data-driven insight to deliver continuous improvements

Get the most from your ISO/IEC 27701 investment with BSI Connect, our integrated technology solution, that helps you effectively plan, manage and drive performance. With preconfigured ISO content, it gives you the tools and insights necessary to manage essential elements of your PIMS.

The start of your ISO/IEC 27701 journey is an ideal time to implement BSI Connect and benefit from:

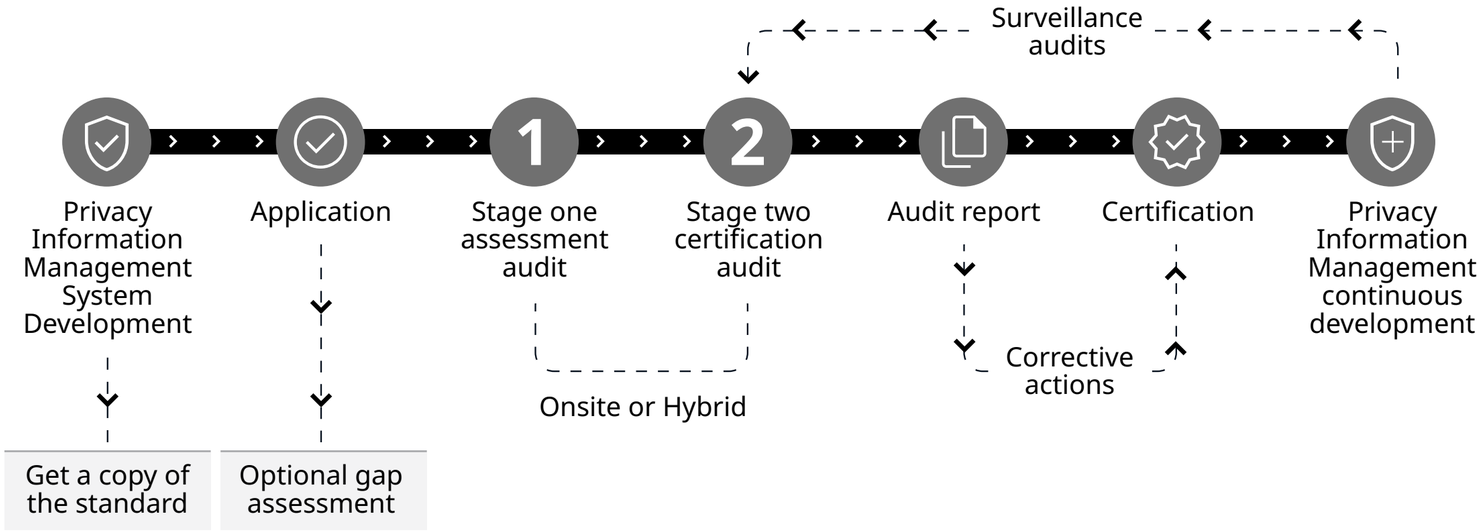
- Plan and track your training needs and activities needed to get to audit stage
- Assign roles and responsibilities related to your privacy information management
- Plan your internal and external audits across your locations
- Manage and get visibility on the progress and performance of your audits

Getting certified is just the beginning of your journey to digital trust

ISO/IEC 27701’s focus on continuous improvement means certification is the first step on your journey to enduring digital trust.

Certification proves to stakeholders that your organization emphasizes and prioritizes protecting sensitive data.

It demonstrates you have taken accountability for processing PII in a secure and compliant way. And it instils confidence that when they do business with you both their data and their reputation is safe in your hands.



BSI Connect

Capture and manage your audits, findings, incidents and risks

Why BSI?

For more than 120 years, BSI has championed what good looks like and driven best practice in organizations around the world. This includes the production of BS 7799, now ISO/IEC 27001, the world's most popular information security standard. And we haven't stopped there, addressing the emerging issues such as cyber, cloud security and privacy with ISO/IEC 27701. That's why we're best placed to be your trusted partner.

With the technical know-how and network of industry experts, academics and professional bodies, we are committed to drive the privacy agenda for both organizations and society.

About BSI

BSI shapes, shares and embeds best practice, so that organizations can become future ready – by being trusted, resilient and ready to succeed in our ever-changing world. By assessing and certifying against standards, regulation, and consensus best practices, we are a catalyst for positive change, creating an enduring legacy of improvement for our clients, their customers, and society.

Call us: +971 4 870 9300
E-mail us: bsi.me@bsigroup.com