bsi.

...making excellence a habit.™

ISO/IEC 27701
Privacy Information Management

Your implementation guide

What is ISO/IEC 27701?

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

It provides guidance and requirements on the protection of privacy, helping both personally identifiable information (PII) processors and PII controllers to put robust data processes and controls in place. This means you can demonstrate accountability for managing PII, instil trust and build strong business relationships.

Contents

What kind of organizations can benefit from ISO/IEC 27701?

ISO/IEC 27701 is ideal for all types and sizes of organizations who want to demonstrate that they take protecting personal information seriously.

Whether you're a public or private company, government entity or not-for-profit organization, if your organization is responsible for processing PII within an information security management system then ISO/IEC 27701 is for you.

Specific organizational roles include:

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

Benefits of ISO/IEC 27701

The key requirements of ISO/IEC 27701

Clause 1: Scope

This 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 in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002. Focused on 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

This clause 'sets the scene' for ISO/IEC 27701. It provides an overview of the documents structure and indicates, at a high-level, the location of PIMS specific requirements in relation to 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.

Detailed guidance on helping your customer respond to individual requests, managing temporary files created during processing, returning, transferring or disposing PII securely and appropriate transmission controls are included.

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 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 2900 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 fulfil 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

BSI is a world leader in helping clients develop the knowledge and skills they need to embed excellence in their organizations. Whether your organization is going to certify or is simply looking to implement a privacy information management system, our training courses will help you embed the knowledge and maximize your ISO/IEC 27701 performance.

ISO/IEC 27701 courses include:

ISO/IEC 27701 Requirements

- One day
- Learn what a PIMS is and understand the ISO/IEC 27701 requirements

ISO/IEC 27701 Implementation

- Two days
- Get the skills to implement an ISO/IEC 27701 privacy information management system

ISO/IEC 27701 Internal auditor

- One day
- As an existing ISO/IEC 27001 auditor, learn how to conduct audits against ISO/IEC 27701

BSI Business Improvement Software

Gain insight and deliver continual improvements

Ensure you get the most from your ISO/IEC 27701 investment with our Business Improvement Software – a solution that can help you effectively manage your privacy information management system. With pre-configured ISO content, it gives you the tools and information necessary to manage essential elements of your PIMS.

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

- Effective document control
- Visibility of site and certificate performance
- Ability to log, track and manage actions related to audits, incidents/events, risk and performance
- Insight into trends that help you make business decisions to drive improvement through its customizable dashboards and reporting tools

Why BSI?

By Royal Charter

ISO/IEC 27701 Privacy Information Management

For over a century 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 new emerging issues such as cyber, cloud security and now privacy with ISO/IEC 27701. That's why we're best placed to help you.

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 is the business improvement company that enables organizations to turn standards of best practice into habits of excellence. Working with over 86,000 clients across 193 countries, it is a truly international business with skills and experience across a number of sectors including automotive, aerospace, built environment, food, and healthcare. Through its expertise in Standards Development and Knowledge Solutions, Assurance and Professional Services, BSI improves business performance to help clients grow sustainably, manage risk and ultimately be more resilient.

To learn more, please visit: bsigroup.com/en-za

bsi.

Find out more
Call: +27(0)12 004 0279
E-mail: bsi.za@bsigroup.com

BSI/UK/1651/SC/1119/EN/GRP