LRQA

ISO 27701: Integrating your information security and privacy management systems

As organizations continue to become more data-rich and reliant on personal information, the importance and complexity of addressing privacy requirements grows. In the eyes of customers, colleagues and other stakeholders, privacy is a non-negotiable expectation.

Failures to protect personal and sensitive information are widely reported, with the volume of data breaches continuing to increase. In most cases, they are highly damaging both in terms of reputation and regulatory compliance.

ISO 27701 provides a solution that helps organizations to implement best practice privacy management, enabling them to meet extensive customer, contractual and legal obligations.

Agustin Lerma Gangoiti
IT Technical Specialist | LRQA

> “We are now in an era where people want more control over their information - they want clarity around how it is used and demand it is protected. These expectations are supported by a growing list of laws and regulations. Organizations now need to respond by ensuring that data privacy is addressed through their management systems and processes on an ongoing, evolving basis.”

ISO 27701 - the future of privacy

ISO 27701 is the first international standard that defines the requirements for a privacy information management system (PIMS). It is an extension to ISO 27001, the framework used by organizations worldwide to implement comprehensive information security management systems (ISMS).

The relationship between ISO 27001 and ISO 27701

ISO 27701 has been developed to integrate with ISO 27001 – you can’t be audited against ISO 27701 in isolation. The link between the two standards helps maintain the end-to-end relationship between information security and privacy.

In practice, ISO 27001 remains the foundation of an information security approach, and ISO 27701 builds on that with a comprehensive set of privacy-specific controls and requirements.

This level of integration avoids the complexity associated with operating multiple standalone systems, and organizations can also choose to integrate with other popular schemes like ISO 22301 and ISO 9001 to drive further efficiencies.

The benefits of best practice data privacy

Laws and regulations like the EU GDPR and Data Protection Act require businesses to implement measures around privacy. However, they don’t provide much detail on how that should be done. ISO 27701 has been developed by ISO (the International Standards Organisation) and IEC (International Electrotechnical Commission) to provide more detailed guidance to fill this gap.

Both ISO 27001 and ISO 27701 require businesses to identify and manage relevant legal requirements. Although an ISO 27701 certified PIMS cannot solely guarantee compliance with a law or regulation, it can provide excellent documentary evidence to supervisory authorities around how an organization manages data processing. This information can also be crucial in enabling agreements with customers, partners and suppliers when products or services exchanged use personal data.

An ISO 27701 PIMS certified by a reputable third party can distinguish an organization from its competition by demonstrating to internal and external stakeholders that privacy is a priority. The framework set out by ISO 27701 enables organizations to more effectively satisfy requirements dictated by both law and good business practice.

Continual improvement

Much like the privacy threat landscape, an ISO 27701 certified PIMS does not remain static. As with all ISO standards, continual improvement is a central theme that helps ensure that the PIMS is continually evaluated and optimized to mitigate risks.

Benefits of ISO 27701 certification

Protect personal information, build trust and clearly define roles and responsibilities

Identify and manage legal requirements

Create a more robust and effective integrated system

Generate a commercial advantage by demonstrating a commitment to best practice privacy management

Getting certified to ISO 27701

Almost all organizations manage personal information and are subject to privacy laws and regulations. As a result, ISO 27701 is an effective tool for any company and is particularly popular with those handling highly sensitive data.

Most businesses choose to have their PIMS certified against ISO 27701 by an independent third party, like LRQA. Third-party certification adds credibility and shows stakeholders that systems have been developed in line with internationally recognized best practice.

Defining your management role

Personal data processing is a very broad term. If you perform any activities relating to personal data, that is classed as processing, and you're subject to legal and moral obligations around what you do and how you do it.

ISO 27701 outlines specific guidance and controls for both Personally Identifiable Information (PII) 'controllers' and 'processors'. Organizations implementing an ISO 27701 PIMS will need to identify whether one or both of these roles apply to them. This is then included in the context of the organization.

PII controller

The person or entity that decides 'how' and 'why' personal data is collected

PII processor

The person or entity who processes data on behalf of the 'controller'

Example

Company A collects personal information from its clients and uses it for marketing purposes. Company A also defines why and how they collect the information and ensures that clients have provided consent. Company A is, therefore, the **controller.**

Company B is a supplier to Company A and provides email marketing services – making them a **processor** of personal information.

PIMS specific requirements

Clause 5 of the ISO 27701 standard covers the requirements of the PIMS.

It addresses the clauses already defined in ISO 27001, such as context, leadership and risk management, and extends them to cover privacy protection. Companies must define their role as a controller and/or processor as part of the context of their organization, as well as identifying any external factors, privacy regulations and contractual obligations that need to be addressed.

Privacy risk management

Clause 6 covers specific guidance for PIMS related to ISO 27002; it goes through each of ISO 27001 Annex A's fourteen control areas and provides implementation guidance on additional control requirements. It is a crucial driver behind effective privacy risk mitigation.

In total, 32 new controls feature within clause 6 that amend ISO 27002. These additional controls require organizations to consider how information security policies should incorporate privacy statements that address compliance, contractual obligations, and stakeholder requirements. There's also added detail around incident reporting, access management and roles and responsibilities relating to the processing of personal information.

Additional requirements for controllers

An organization aiming to be certified as a ‘controller’ will need to consider the guidelines set out in clause 6, plus specific guidance covered by clause 7, which relates to controls listed in Annex A.

Annex A includes 31 controls specific to controllers that focus heavily on collecting and processing personal information, obligations to PII principals, and implementing privacy-by-design. These controls are mandatory unless a justification for exclusion is provided via the statement of applicability.

Additional requirements for processors

Clause 8 outlines specific guidance for processors and relates to the controls listed in Annex B.

There are 18 specific controls for processors that address key areas, including record keeping, responding to requests, and sharing, transferring and disclosing personal information. These controls are also mandatory unless the organization in question justifies their exclusion in the statement of applicability.

Clauses	# of Annex A controls (Controllers)	# of Annex B controls (Processors)
Conditions for collection and processing	8	6
Obligations to PII principals	10	1
Privacy by design and privacy by default	9	3
PII sharing, transfer and disclosure	4	8

Optimizing your audit

LRQA provides audit and certification services against ISO 27701.

As ISO 27701 is not a standalone standard and integrates with ISO 27001 - the most efficient option is to be audited against both simultaneously. An integrated audit provides several efficiencies, such as improved planning and less duplication, which, in some cases, can lead to a reduction in overall audit duration.

For organizations already certified to ISO 27001, the ISMS scope will need to be equal to or greater than that of the PIMS. An organization’s PIMS will need to cover all business areas that access or process personal information, whereas an ISMS only typically focuses on a few key departments such as IT and facilities.

Why choose LRQA?

We're here to help negotiate a rapidly changing world, by working with you to manage and mitigate the risks you face. From compliance to data-driven supply chain transformation, it's our job to help you shape the future, rather than letting it shape you. We do this by delivering:

Strategic vision

Our technical know-how, sector expertise and innovative, forward-thinking approach will help you meet the challenges of today – and become a safer, more secure, and sustainable organization tomorrow.

Technical expertise

Our people are sector experts. They bring with them a clear understanding of your specific challenges, standards and requirements – then deploy deep knowledge of certification, customized assurance, cybersecurity, inspection and training to help you meet them.

Global capability

Operating in more than 120 countries, recognized by over 50 accreditation bodies worldwide, and covering almost every sector, we can help you manage risk, drive improvement and build credibility with stakeholders around the globe.

Effective partnership

Every business is unique. That's why our experts work with you, to fully understand your needs and goals, and work out how we can best support them.

Fresh perspective

We have led the way in shaping our industry and continue to take every opportunity to collaborate with clients and pioneer new ideas, services and innovation.

Get in touch

For more information, visit **lrqa.com/us**

LRQA

YOUR FUTURE. OUR FOCUS.

About LRQA:

By bringing together unrivaled expertise in certification, brand assurance, food safety, cybersecurity, inspection and training, we've become a leading global assurance provider.

We're proud of our heritage, but it's who we are today that really matters, because that's what shapes how we partner with our clients tomorrow. By combining strong values, decades of experience in risk management and mitigation and a keen focus on the future, we're here to support our clients as they build safer, more secure, more sustainable businesses.

From independent auditing, certification and training; to technical advisory services; to real-time assurance technology; to data-driven supply chain transformation, our innovative end-to-end solutions help our clients negotiate a rapidly changing risk landscape – making sure they're shaping their own future, rather than letting it shape them.

Get in touch

Visit **www.lrqa.com/us** for more information
866-971-LRQA
info-usa@lrqa.com

1330 Enclave Parkway, Suite 200
Houston, TX 77077
United States

Care is taken to ensure that all information provided is accurate and up to date; however, LRQA accepts no responsibility for inaccuracies in or changes to information.

For more information on LRQA, click **here**.