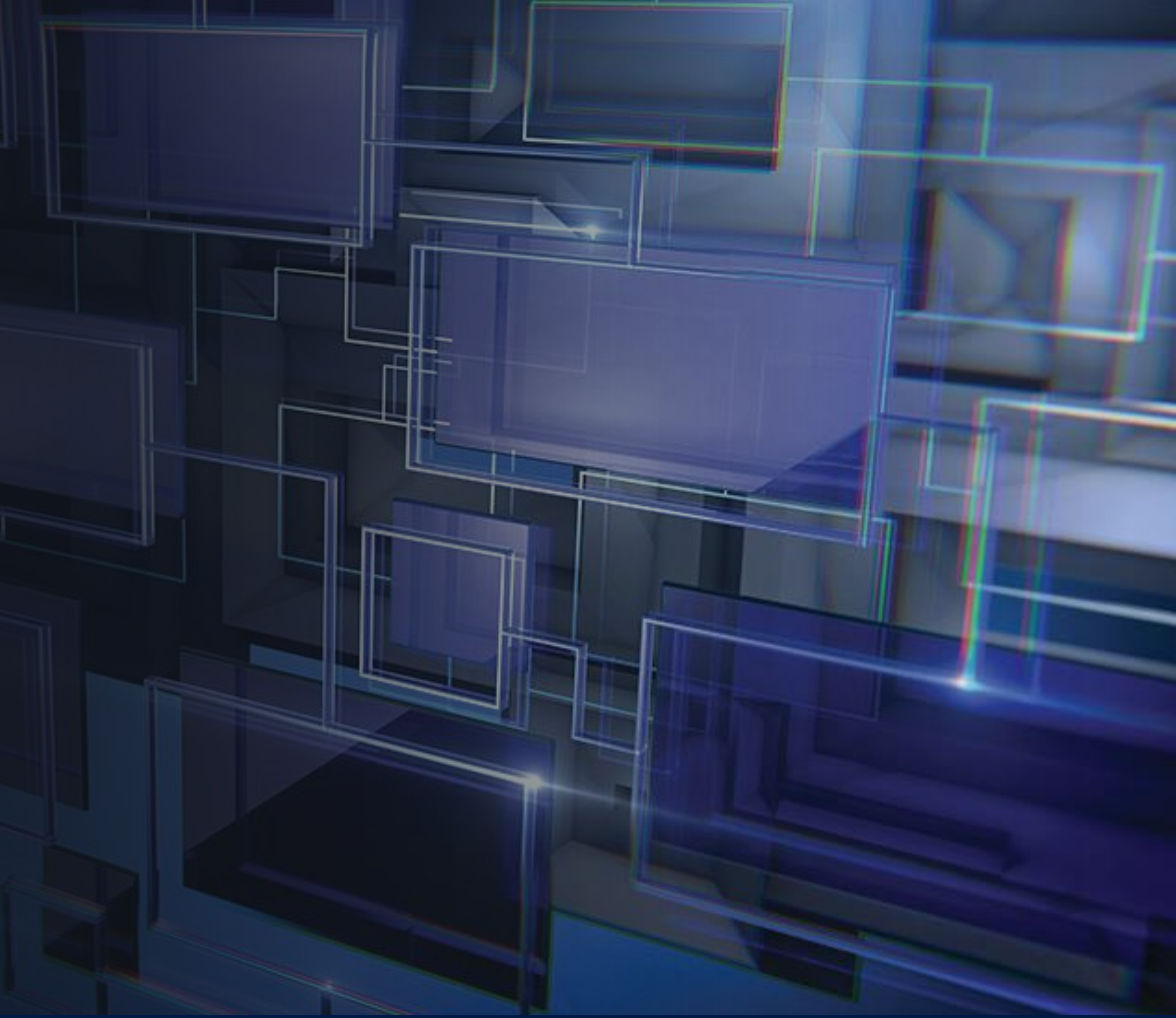
Management Solutions
Making things happen

Technical note on

ISO/IEC 27701:2025

Information security, cybersecurity and privacy protection

Note: ISO 27701:2025 is a private standard. This summary is exclusively based on public official information.



1. Executive summary

2. Main content

3. Main definitions

4. Why MS?

A. Annex

1 Executive summary

General overview

ISO/IEC 27701:2025 was published on the 14th of October 2025, aiming at strengthening privacy protection by defining a structured Privacy Information Management System (PIMS)

Context

- **In 2019,** the International Organization for Standardization (ISO) published the **first edition of ISO/IEC 27701:2025,** establishing a framework for managing privacy in Personally Identifiable Information (PII) processing.
- Since then, organizations have **increasingly processed large and varied amounts of PII**, across multiple jurisdictions, while privacy has become a growing societal expectation and the focus of expanding regulatory frameworks worldwide.
- In this context, ISO **has updated ISO/IEC 27701:2025 with a technically revised second edition to reinforce accountability and provide a consistent and verifiable approach to PII protection.**

Scope

- **Specify requirements** for establishing, implementing, maintaining, and continually improving a PIMS.
- **Support organizations** in managing privacy risks, enhancing accountability, and building trust with stakeholders.

Alignment with other standards

- Builds on **ISO/IEC 27001:2025** (information technology), setting out privacy-specific extensions to the Information Security Management System.
- Aligns with **ISO/IEC 29100:2024** (privacy framework and principles), **ISO/IEC 27018: 2025** (PII protection in cloud environments), and **ISO/IEC 29151:2017** (PII protection controls).
- Ensures **consistency with** the European Union (EU) **General Data Protection Regulation (GDPR)** and other global privacy regulations, reinforcing accountability and governance requirements.

Main content

Elements for a more comprehensive and modernized PIMS

- Reinforce privacy policies and objectives, risk and responsibility management, the establishment of operational controls to protect information, the monitoring of system performance, and the assurance of continuous improvement.

Guidance on privacy risk management, regulatory compliance and demonstration of accountability

- Guidance on how to implement controls, measure their performance, and document evidence of compliance has been expanded. This seeks to facilitate agreements and relationships with business partners, as well as evidence of good practices in the processing of PII.

Who can use it?

Organizations accountable for the processing of PII, requiring a structured and verifiable approach to privacy protection

- The document is intended for PII controllers and PII processors holding responsibility and accountability for PII processing.
- In addition, it is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations.

Access to more detail

2 Main content

ISO/IEC 27701:2025 framework structure

ISO/IEC 27701:2025 provides a structured framework to extend information security management with privacy controls, ensuring protection of personal data, clear responsibilities and compliance across the organization

Contents

1. Scope

2. Normative references

3. Terms, definitions and abbreviations

4. Context of the organization

5. Leadership

6. Planning

7. Support

8. Operation

9. Performance evaluation

10. Improvement

1 **Type of PIMS** to which it applies; the **organizations** it covers; and the **objectives** to be achieved through its implementation.

2 **Normative documents** necessary for the standards **interpretation or application**.

3 The specific terms, definitions, and abbreviations used in the standard.

4 Determines **organization's role** as a PII controller or PII processor, identifies **external and internal factors** that may affect its PIMS, and defines its scope.

5 **Commitments of top management** to define privacy policies, assign **roles and responsibilities**, and ensure that the PIMS is **integrated into** the organization's **processes**.

6 Actions to address **risks and opportunities**, to define **privacy objectives**, and to design how the **system's requirements** will be integrated into the business.

7 The **resources, competencies, awareness, communication, and document control** necessary to effectively operate and maintain the PIMS.

8 The execution of **planned processes, operational control, management** of risk treatment, and the handling of personal data in the organization's activities.

9 How the organization should **monitor, measure, analyze, and evaluate the performance** of the PIMS, including internal audits, management reviews, and compliance monitoring.

10 Identify **opportunities for improvement**, address nonconformities, and continually enhance the organization's privacy information management system.

3 Main definitions

Specific terminology of ISO/IEC 27701:2025

ISO/IEC 27701:2025 uses common management system terminology from ISO standards and introduces additional definitions specific to privacy governance and PIMS

Specific Term	*Explanatory Definition*
PII	Information that identifies or can be used to identify a natural person, directly or indirectly, and whose processing may affect privacy.
PII Controller	Organization determining the purposes and means of PII processing and accountable for privacy protection.
Joint PII Controller	Two or more controllers jointly determining purposes and means of the processing of PII and sharing accountability.
PII Processor	Organization processing PII on behalf of a controller and acting under its instructions.
PIMS – Privacy Information Management System	Set of interrelated elements for managing privacy risks related to PII processing and demonstrating responsible practices.
Statement of Applicability (SoA)	Documentation identifying applicable privacy controls and justification for their inclusion/exclusion within the PIMS.

4 Why MS?

Credentials and Differential Value

Management Solutions has a multi-sectoral and in-depth knowledge of the main stakeholders, as well as strong capabilities and accelerators to achieve practical results in an agile manner

Proven experience in Technological Risk and Cybersecurity projects

Value offer in technological risk management and cybersecurity that combines knowledge of three specific areas (technological cybersecurity, IT risk assessment and business), creating a mixed profile that allows covering various areas of high demand:

- **Governance, Risks and Compliance**: assessment, risk appetite and digital resilience strategy, organization and governance, development/updating of regulatory bodies, PMOs for IT Risk and Cybersecurity programs, support in audit/inspection and certification processes, definition and application of frameworks and methodologies (e.g. for risk quantification based on scenarios / Stress Tests), …
- **Implementation of controls**: training and awareness plans, crisis management, access control, management of IT and cybersecurity risks with third parties, data security, support in the selection of services and solutions, …
- **Execution of services and operation of controls**: Cybersecurity Offices (CISO Support), IT Risk Offices (2LoD Support), …

Proven experience in ICT Risk projects

- Value proposal in ICT risk management that combines knowledge of three specific areas (technological cybersecurity, ICT risk assessment and business), creating a mixed profile that allows us to cover various areas of high demand.
- **Governance, Risk and Compliance**: assessment, risk appetite and digital resilience strategy, organization and governance, development/updating of regulatory bodies, PMOs of ICT risk programs, support in audit/inspection and certification processes, definition and application of frameworks and methodologies…
- **Implementation of controls**: training and awareness plans, crisis management, access control, Third-Party ICT Risk management, **data security**, support in selecting services and solutions.
- **Execution of services and operation of controls**: Cybersecurity Office (CISO/BISO Support), ICT 2LoD Office, Third-Party ICT Risk Office, Digital Operational Resilience Office.

High-value profiles, expertise and cross vision

- Professionals with strong **understanding, communication, challenge/high-value advice, expertise in ICT risks and their relation to risk management and processes (cross vision).**
- Understanding of **business processes**, knowledge of **risk management** methodologies **and strong analytical skills.**
- **Detailed knowledge of market regulations, standards and best practices** (COBIT, ISOs, GDPR, NIST, ITIL, SANS, DORA, EBA GL, NIS2, CSF, CSA ...).

Benchmark firm with global capabilities

- **One global Firm, independent and international** (+50 countries), with in-depth knowledge of the businesses in which our clients operate (+2,000 global and local) selecting the most appropriate resources for each project, regardless of where they are located.
- **Multidisciplinary team** with strong analytical skills and specialist knowledge. Organized on a matrix basis (customer, industry, competitor and geography).
- Consultant accredited by **supervisors and supranational bodies** (ECB, FCA, PRA, BoE, BNH, BNG, BNS, BNM, SBIF, SBS, BCCR, SSN, EIOPA, etc.).
- **A strong corporate culture**: commitment, dedication to service and a constant search for excellence.
- **A proven track record**, which has resulted in significant organic growth (x50 in 21 years) **benchmarking** capability (presence at top clients in all geographies).

Access to regulatory and supervisory criteria

- We assist **supervisors in their on-site inspections** in organizations.
- **We directly support organizations in overcoming on-site monitoring, internal and external audit processes** in the area of ICT risks.
- **Office in Frankfurt as Hub for regulatory analysis and liaison with the regulator** for regulatory issues, queries and anticipating requirements.

A Annex
Abbreviations

Abbreviation	Meaning
EU	European Union
GDPR	General Data Protection Regulation
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
PII	Personally Identifiable Information
PIMS	Privacy Information Management System
ISMS	Information Security Management System
SoA	Statement of Applicability
ICT	Information and Communication Technology
PMO	Project Management Office
CISO	Chief Information Security Officer
BISO	Business Information Security Officer

Management Solutions

Making things happen

International
One Firm

Multiscope
Team

Best practice
know-how

Proven
Experience

Maximum
Commitment

Alejandro Iglesias
Partner at Management Solutions
Alejandro.Iglesias@msspain.com

Marta Hierro
Partner at Management Solutions
Marta.Hierro@msspain.com

The information contained in this publication is merely to be used as a guideline, is provided for general information purposes and is not intinged to be used in lieu of consulting with our professionals. Management Solutions is not liable for any use that third parties may make of this information. The use of this material is not permitted without the express authorization of Management Solutions.

For more information please visit

www.managementsolutions.com

Or follow us at: