TEVORA™ | White Paper

ISO/IEC 27701:2019 Compliance Guide

Derek Glausser
April 12, 2023

Table of Contents

Glossary of Terms

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

A documented management system consisting of a set of security controls that protect the confidentiality, availability, and integrity of assets from threats and vulnerabilities.

JOINT PII CONTROLLER

PII controller that determines the purposes and means of the processing of PII jointly with one or more other PII controllers.

PERSONAL IDENTIFIABLE INFORMATION (PII)

Any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person.

PII CONTROLLER

Privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information.

PII PRINCIPALS

A natural person to whom the personally identifiable information (PII) relates, often referred to as data subjects.

PII PROCESSOR

Privacy stakeholder that processes personally identifiable information on behalf of and by following the instructions of a PII controller

PRIVACY INFORMATION MANAGEMENT SYSTEM (PIMS)

Information security management system which addresses the protection of privacy as potentially affected by the processing of PII.

FOR MORE TERMS AND DEFINITIONS RELATED TO ISO/IEC:

ISO Online Browsing Platform is available at iso.org/obp
IEC Electropedia is available at electropedia.org

Introduction

Privacy protection legislation is sprouting up all around the world, including amongst individual states in the U.S. It can be overwhelming for organizations that work globally and even across the United States to keep up with these laws, let alone comply with them. This trend in legislative policies has mainly been driven by consumers becoming conscious of the value and size of their digital footprint. This privacy consciousness can be leveraged by organizations that substantively address privacy as a distinctive feature of their product or service. Personal Identifiable Information (PII) protection has the interconnected benefits of lowering organizational risks associated with personal data while also bolstering customer trust.

As an organization grows, its PII environment tends to trend towards complexity. Thus, organizations can lower the amount of time and resources needed to protect their PII the sooner they address it. Additionally, an organization without a robust system underlining existing and future PII processing operations will have an increasingly difficult time addressing its privacy needs.

Although there are many independent privacy laws, your organization's response does not have to be splintered. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) bodies published the ISO/IEC 27701:2019 framework to help an organization comply with all their contractual, legal, and regulatory obligations regarding the processing of PII under one system. A Privacy Information Management System created under the guidance of ISO/IEC 27701:2019 is a big step forward for any organization wishing to address privacy risks effectively and efficiently.

Tevora has created a Privacy Tracker to help organizations keep up to date with privacy laws.

What is ISO/IEC 27701:2019?

ISO/IEC 27701:2019 simply put is a guide to extending an organization's information security management system to consider the protection of PII principals. The end goal of becoming ISO/IEC 27701:2019 certified is to have a robust Privacy Information Management System (PIMS) that addresses all applicable contractual, legal, and regulatory obligations regarding the processing of personal information. It is designed to be an enhancement to information security management systems created under the guidance of ISO/IEC 27001:2013 and ISO/IEC 27002:2013.

This framework is versatile and can help organizations of all types and sizes that interact with PII. Fulfilling the requirements and complying with ISO/IEC 27701:2019 will give organizations a cerebral understanding of how they process personal information. It will also provide substantive evidence that can be used to facilitate agreements with business partners where the processing of personal information is jointly relevant. This evidence can also be used to help demonstrate compliance with data protection laws and regulations such as the General Data Protection Regulation (GDPR) when implemented controls are mapped to applicable laws and regulations.

PIMS created under this framework can be either a separate system alongside an existing ISMS, or it can be integrated into an existing security management system. While the framework works off the assumption that an ISMS has already been established. It is possible to create both systems in a condensed timeframe. This approach would stagger the ISO/IEC 27001:2013 certification process to start before the ISO/IEC 27701:2019 certification process. Allowing the foundational aspects of ISO/IEC 27001:2013 to have been established and then implementing the needed additions required by ISO/IEC 27701:2019.

Why Should We Seek ISO 27701:2019 Certification?

BUILDS TRUST

Achieving 27701 certification demonstrates to your customers, clients, and partners that you take privacy seriously and helps them trust that you will protect their sensitive information. You can use your 27701 certification status as a key ingredient in your advertising, marketing materials, website content, and client communications to reinforce your commitment to data privacy.

CIRCUMVENTS PRIVACY AUDITS

In some cases having an ISO 27701 certificate will circumvent the need for an independent privacy audit. For example, Microsoft requires most suppliers to undergo an independent privacy audit, but if you are ISO 27701-certified, they may waive this requirement.

IMPROVES PUBLIC PERCEPTION

As privacy concerns have significantly escalated in recent years, having an ISO 27701 certificate can go a long way toward improving the public's perception regarding the privacy practices of your organization.

PROVIDES COMPLIANCE MAPPING

Having an ISO 27701-compliant PIMS will help your organization comply with most international data privacy regulations. Achieving 27701 compliance establishes a framework that covers most legal privacy requirements. With that said, you should expect some incremental work to comply with certain caveats and nuances of specific privacy regulations in different geographic regions.

Key Aspects of ISO/IEC 27701:2019

PROCESSORS AND CONTROLLERS

This framework breaks down organizations into either controllers or processors and provides guidance specific to each instance. Controllers can be understood as the organization that determines the 'how' and 'why' of PII processing. Controllers can conduct all processing in-house, or they can delegate tasks to another entity. When controllers delegate, they create the position of the processor. Processors are entities that follow the processing guidelines set out by the controller and perform processing activities on their behalf.

There is a less common relationship in PII processing called joint controllers. This occurs when a PII controller determines the purposes and means of processing with one or more other PII controllers.

PRIVACY IMPACT ASSESSMENTS (PIA)

This framework recommends organizations should define and determine when a PIA is needed. It is most commonly needed whenever new processing of PII occurs or changes to existing processing of PII are planned.

Depending on the jurisdiction and type of the PII processing, a privacy impact assessment may be required.

Privacy Impact Assessments are recommended to do the following:

- Describe the nature, scope, context, and purposes of the processing of PII
- Assess necessity, proportionality, and compliance measures
- Identify and assess risks to PII principals
- Identify any additional measures needed to mitigate those risks

PRIVACY BY DEISGN AND DEFAULT

"Privacy by Design" is "data protection through technology design." This means proactively integrating data privacy into the design, operation, and management of a system. Technology is constantly increasing in complexity and scope, therefore a system that was designed from the start to promote privacy will more effectively and efficiently meet compliance standards than a reactionary system. Data protection regulations like the GDPR consider "Privacy by Design" as one of the most important aspects of data protection. "Privacy by default" is the process of incorporating privacy from the start.

The purpose of these principles is to ensure that processes and systems are designed such that the collection and processing (including use, disclosure, retention, transmission, and disposal) are limited to what is necessary for the identified purpose.

What has been added to the ISO/IEC 27001:2013 controls?

Significant Changes

The 'Context of the Organization', and 'Planning' domains receive the most additions in this section.

'Context of the Organization' changes circumscribe around expanding the organization's perspective to include the right amount of attention to privacy-related factors that are relevant to its context and that can affect the intended outcomes of its PIMS. Such as privacy legislation, regulations, judicial decisions, etc. The first step in this process for any organization that processes PII is to determine its role as a PII controller (including as a joint PII controller) and/or a PII processor.

In tandem with this expansion, organizations must now revamp their interested parties determined under ISO/IEC 27001:2013. This new search must include any parties that have interests or responsibilities associated with the processing of PII, including the PII principals. Other interested parties can include customers, supervisory authorities, other PII controllers, PII processors, and their subcontractors.

These additions underly the overall process of determining the scope of the PIMS. ISO/IEC 27701:2019 has the obvious inclusion that the processing of PII must be included in the scope. The framework recommends revising the scope of the information security management system, because of the extended interpretation of "information security".

Following the determination of scope, is the question of integration. Whether the PIMS should be a separate system or integrated into an existing ISMS. The answer is relative to the management and organizational needs, but either way, the organization must establish, implement, maintain, and continually improve the PIMS following the requirements of ISO/IEC 27001:2013 Clauses 4 to 10.

The 'Planning' section focuses on the risk assessment and treatment processes incorporating PII processing risks. The framework calls for an information security risk assessment process to identify risks associated with the loss of confidentiality, integrity, and availability, of PII within the scope of the PIMS. To do this properly, organizations must manage the relationship between information security and PII protection. This includes assessing the potential consequences for both the organization and PII principals.

Parallel to the expansion of the scope is the expansion of the Statement of Applicability. It must be extended to contain justifications for the inclusion or exclusion of the controls listed in ISO/IEC 27701:2019 Annex A and Annex B. Not all of the control objectives and controls listed in the annexes need to be included in a PIMS implementation. Justification for exclusion can include where the controls are deemed unnecessary.

Minimal Changes

The 'General' section adds that wherever the term "information security" is used within an existing ISMS, is to be extended to include the protection of privacy as potentially affected by the processing of PII.

No Changes

'Leadership', 'Support', 'Performance Evaluation', and 'Improvement' sections receive no additions.

What has been added to the ISO/IEC 27001:2013 controls?

The following bullet points describe the additional implementation measures that need to be taken in addition to those created under the guidance of ISO/IEC 27002:2013.

GENERAL

As stated in the 'General' section above, wherever information security is mentioned in the existing ISMS the term should be extended to include the protection of privacy. In practice, it is a policy change, best practices recommend changing the term "information security" to"information security and privacy.

INFORMATION SECUIRTY POLICIES

The Leadership and Commitment statement created for an ISMS should be extended to account for compliance with applicable PII protection legislation, regulations, and contractual agreements.

This attention should be given throughout the development and maintenance of all information security policies.

ORGANIZATION OF INFORMATION SECURITY

Information security roles and responsibilities - an organization should create a point of contact (POC) for customers regarding the processing of their PII. If the organization is a PII controller, it should create a POC for PII principals regarding the processing of their PII. The framework also provides specific criteria regarding the POC.

Mobile device policy - organizations must implement controls that ensure mobile devices do not lead to a compromise of PII. This can take the form of technical and personnel-oriented controls.

HUMAN RESOURCE SECURITY

During employment - Information security awareness, education, and training - Personnel should be made aware of the possible consequences to the organization, to themselves, and the PII principal in response to breaching privacy or security rules and procedures, especially those addressing the handling of PII.

Such measures could be the teaching of how to report incidents.

ASSET MANAGEMENT

Classification of information - Information classification systems should explicitly show consideration of PII as part of the system it implements. This consideration is vital for a clear and current understanding of PII processing and storing operations.

Labelling of information Personnel should be made aware of the definition of PII and how to recognize data that is PII.

Management of removable media The use of removable media and/or devices for the storage of PII should be tracked and documented. Encryption should be used on these devices whenever feasible.

Disposal of media Secure disposal procedures should be created and maintained that specifically relate to devices that processed or stored PII.

Physical media transfer When physical media is used for information transfer, a robust tracking and documentation system should be put in place. Encryption should be used on these devices whenever feasible.

ACCESS CONTROL

User registration and de-registration The framework calls for extra attention to be given to procedures for registration and de-registration of users. These policies should take special precautions for users who administer or operate systems, such as unique IDs for all accounts and never reissuing de-activated or expired user IDs.

User access provisioning An accurate, up-to-date record of users with access to IT systems with PII should be maintained. This is most commonly done by creating unique user IDs and tracking when they access the system.

User responsibilities Secure log-on procedures- When requested by the customer, the organization should provide the ability for secure log-on.

CRYPTOGRAPHY

Policy on the use of cryptographic controls A Cryptography Policy should also account for sensitive data that legally require the use of cryptography. Best practices also call for providing information to the customer regarding the circumstances in which it uses cryptography to protect the PII it processes.

PHYSICAL AND ENVIRONMENTAL SECURITY

Secure disposal or re-use of equipment If storage space is re-assigned, any PII previously stored on it should be verified to not be accessible. If deletion of PII is impractical due to perforamcne issues mitigating technical controls should be implemented. Any device that has the potential to contain PII should be treated as if it does.

Clear desk and clear screen policy Hardcopy material with PII should be restricted and only created when necessary.

OPERATIONS SECURITY

Information backup organizations should create a policy to address the backup, recovery, and restoration of PII. Additionally, it should cover the requirements for the erasure of the PII contained in these backups.

Event logging Organizations should create a process that reviews event logs. This process should be continuous, with automated monitoring and alerting. If this is not feasible then the reviews should be conducted manually.

Protection of log information Some log information can contain PII, so measures to control access to them should be put in place. Additionally, a procedure, preferably automatic, should be put in place to ensure that logged information is either deleted or de-identified as specified in the retention schedule.

COMMUNICATIONS SECURITY

Information transfer policies and procedures It is recocmed to create procedures that ensure that rules related to the processing of PII are enforced internnaly and externally of the system, where applicable.

Confidentiality or non-disclosure agreements Personnel with access to PII are subject to a confidentiality obligation. This agreement should specify the length of time and the obligations required of the employee. This can be included in a empoyment contract or done separtly.

SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE

Securing application services on public networks If unavoidable, when PII is transmitted over untrusted networks, it should be encrypted in transit. This includes any facility that is outside the control of the organization.

Secure development policy Privacy by Design and Default should be created for system development. This includes guiding the organization's processing of PII based on obligations to customers, and applicable laws.

Secure systems engineering principles Privacy by Design and Default should be implemented on all systems and components related to the processing of PII.

Outsourced development Outsourced information systems must use the same principles of privacy by design and privacy by default.

Protection of test data PII should be substituted with false or synthetic PII when conducting tests. If unavoidable, proper mitigating measures equivalent to those used in the production environment should be implemented.

SUPPLIER RELATIONSHIPS

Addressing security within supplier agreements Supplier agreements should specify whether PII is processed and the minimum technical and organizational controls that are needed to be met by the supplier to adequately protect the PII.

INFORMATION SECURITY INCIDENT MANAGEMENT

Responsibilities and procedures The overall incident management process should include specific responsibilities and procedures for identifying and recording breaches of PII. Organizations should stay up to date with each jurisdiction they operate in because some impose specific regulations regarding breach responses.

Response to information security incidents When an incident includes PII, the organzation should take steps to review and determine if a response is needed.

INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

No additional implementation guidance.

COMPLIANCE

Identification of applicable legislation and contractual requirements Organizations should take steps to identify any potential legal sanctions related to their processing of PII.

Protection of records Organizations should archive copies of their privacy policies and procedures for the time specified in their retention schedule.

Independent review of information security Organizations acting as a PII processor, where it is impractical for customers to verify security independently, should make available independent evidence that information security is implemented and operated following the organization's policies and procedures Technical compliance review- Organiations should consider PII processing in all technical reviews for compliance with their security policies and standards.

Additional ISO/IEC 27002:2013 guidance for PII controllers and PII processors

The following sections explore specific guidance created for PII controllers and processors. The implementation guidance is documented in Annex A and Annex B respectively.

Conditions for collection and processing

Controllers and processors share the objective to ensure that PII processing is lawful, with a solid legal basis as per applicable jurisdictions, and has clearly defined legitimate purposes for processing. Below discerns how the two sections diverge to accomplish the same goal.

Controller

- **Identify and document purpose** The first step for a controller should be to identify the 'why' of their PII processing and document the rationale.
- **Identify lawful basis** In tandem with the first step should be determining, documenting, and complying with the relevant legal basis identified for the processing of PII.
- **Determine when and how consent is to be obtained** If the controller plans to use consent as their legal basis, they should create a robust process that can show the 'how' and 'why' the consent was collected from the PII principal.
- **Obtain and record consent** Controllers should implement the procedure created above, and track consent for PII processing that was freely given by the PII principals.
- **Privacy impact assessment** Controllers should stay vigilant to changes in existing PII processing activities, or new ones. If changes are planned or detected, they should conduct a privacy impact assessment.
- **Contracts with PII processors** If a controller contracts with any PII processor, they should have a written agreement detailing the implementation of the appropriate controls.
- **Joint PII controller** If a controller is sharing in the decision-making process regarding PII processing with another controller they should determine respective roles and responsibilities.
- **Records related to processing PII** The controller should determine and document any necessary records that can show its support of its obligations for the processing of PII.

Processor

- **Customer Agreement** The contract with the PII Controller should have clear roles and responsibilities for the entity acting as the processor.
- **Organization's purposes** The processor must only process PII for the purposes dictated by the controller.
- **Marketing and advertising use** the processor should not process PII for marketing and advertising purposes without first gaining consent from the PII principal.
- **Infringing instruction** If the processor believes a processing instruction violates applicable laws, they should inform the customer.
- **Customer obligations** The processor should maintain and provide information to customers that can be used by them to verify compliance with obligations.
- **Records related to processing PII** The processor should determine and document any necessary records that can show its support of its obligations for the processing of PII (as specified in the applicable contract).

Obligations to PII principals

Controllers and processors share the objective to guarantee that PII principals are given adequate information about the processing of their PII and are able to act on applicable rights. Below discerns how the two sections diverge to accomplish the same goal.

Controller

- **Determining and fulfilling obligations to PII principals** To fulfill obligations the controller must first determine what they are and document them. These obligations can be a wide variety from legal, and regulatory, to business obligations to PII principals related to the processing of their PII.
- **Determining information for PII principals** Adequate information should be given to PII principals regarding the processing of their PII. To accomplish this controller should determine all relevant information and then document it.
- **Providing information to PII principals** Clear and easily accessible information should be provided to the PII principle identifying the PII controller and describing the processing of their PII.
- **Providing a mechanism to modify or withdraw consent** The controller should notify PII principals of their rights (specific to the jurisdiction) related to withdrawing consent at any time and provide an easily accessible way to do so.
- **Providing a mechanism to object to PII processing** The controller should notify PII principals of their rights (specific to the jurisdiction) to object in certain situations and provide an easily accessible way to do so.
- **Access, correction, and/or erasure** The controller should implement mechanisms to enable PII principals to obtain access to, correct, and erase their PII. And, when they send a request it should be handled without undue delay. There should be defined a response time and a formal fulfillment process.
- **PII controllers' obligations to inform third parties** Third parties to whom the controller has shared PII should inform them if any modification, withdrawal, or objections pertaining to the shared PII has occurred. Formal processes should be created to guide this process.
- **Providing a copy of the PII processed** A copy of their PII should be able to be shared with the PII principal when requested without undue delay.
- **Handling requests** A formal policy and process should be defined for handling and responding to legitimate requests from PII principals.
- **Automated decision-making** If a controller uses automated decision-making, they should be conscious of any additional obligations to PII principals created from this type of processing on PII.

Processor

- The processor should provide the controller with the means to comply with its obligations related to PII principals.

Privacy by design and privacy by default

Controllers and processors share the objective to ensure that processes and systems incorporate collection and processing privacy principles in the design stages and are the default configuration. Below discerns how the two sections diverge to accomplish the same goal.

Controller

- **Limit collection** The controller's collection of PII should be limited to the minimum that is relevant, proportional, and necessary for the identified purposes.
- **Limit processing** The controller's processing of PII should be limited to that which is adequate, relevant, and necessary for the identified purposes.
- **Accuracy and quality** The controller should verify that PII is as accurate, complete, and up-to-date as is necessary for the purposes for which it is processed. This should be documented and maintained throughout the life cycle of the PII.
- **PII minimization objectives** The controller should define data minimization objectives and what controls are used to meet those objectives. It is recommended to keep documentation.
- **PII de-identification and deletion at the end of processing** PII should be deleted or transformed in a way that does not allow identification or re-identification of PII principals. This should occur as soon as the original PII is no longer necessary.
- **Temporary files** The controller should create a robust process to ensure that temporary files containing PII are deleted in a specified timeframe.
- **Retention** PII should not be kept for longer than is necessary for the purposes for which the PII is processed.
- **Disposal** The controller should have robust policies, procedures, and/or technical controls for the disposal of PII.
- **PII transmission controls** The controllers should implement technical controls to ensure data transmission is secure and reliable.

Processor

- **Temporary files** The processor should follow a robust process to ensure that temporary files containing PII are deleted in a specified timeframe.
- **Return, transfer, or disposal of PII** Processors should be able to return, transfer, and/or disposal of PII in a secure way. This policy should be shared with the controller.
- **PII transmission controls** The processor should implement technical controls to ensure data transmission is secure and reliable.

PII sharing, transfer, and disclosure

Controllers and processors share the objective to be conscious of situations where the sharing, transferring, or disclosing of PII would involve new jurisdictions or obligations. These situations should also be documented. Below discerns how the two sections diverge to accomplish the same goal.

Controller

- **Identify the basis for PII transfer between jurisdictions** When transferring PII between jurisdictions the controller should identify and document the relevant basis for them.
- **Countries and international organizations to which PII can be transferred** If there is a possibility of PII being transferred elsewhere the controller should specify and document the potential countries and international organizations of transfer.
- **Records of PII disclosed to third parties** Transfers of PII to or from external parties should be tracked and documented by the controller. This will aid future cooperation and PII principal requests.

Processor

- **Basis for PII transfer between jurisdictions** When transferring PII between jurisdictions the processor should inform the customer in a timely manner of why the PII is being transferred. This is intended to give PII principals the ability to object to the transfer.
- **Countries and international organizations to which PII can be transferred** Any country or international organization that may receive PII that is under the control of the processor should be specified and documented.
- **Records of PII disclosed to third parties** Disclosures of PII to third parties should be recorded. This includes the who, what, when, and where.
- **Notification of PII disclosure requests** The processor should make sure the customer is aware of any legally binding requests for disclosure of PII.
- **Legally binding PII disclosures** Any request for PII disclosures that are not legally binding should be immediately dismissed by the processor. Additionally, processors should consult with their customers before making any PII disclosures, and provide any disclosures agreed upon with their customers.
- **Disclosure of subcontractor to process PII** The processor should be forthcoming about their use of subcontractors to process PII and it should be addressed in the customer contract prior to using.
- **Engagement of a subcontractor to process PII** Processing conducted by subcontractors must stay within the bounds of processing dictated by the controller.
- **Change to a subcontractor to process PII** When processors (with prior written authorization for subcontracting) must add or change their subcontractors that process PII, they should inform the customer and give them time to object.

Author Profile

DEREK GLAUSSER, Senior Information Security Associate

PRIMARY ROLE

Derek Glausser is an Information Security Associate responsible for contributing to various projects within the Privacy team and the ISO 27001 practice at Tevora.

NOTABLE ACCOMPLISHMENTS

Derek possesses a bachelor's degree from the University of Pittsburgh, Pennsylvania, specializing in Economics and Political Science. He leverages his education to have a robust understanding of legal frameworks and regulatory standards related to privacy and security.

CERTIFICATION AND TRAINING

Derek completed a fellowship at Carnegie Mellon University focused on Information Systems and Information Security. Derek is an ISO 27001 Lead Auditor, ISO 27701:2019 Internal Auditor, and is currently working towards a CIPP/E certification.

TENURE

Derek has been with Tevora since May 2021.

About Tevora

Tevora is a leading management consulting firm specializing in enterprise risk, compliance, information security solutions, and threat research. We offer a comprehensive portfolio of information security solutions and services to clients in virtually all industries and also serve institutional and government clients.

Tevora's leaders are professionals with years of experience and records of accomplishments in technology as well as business. This dual background means that we understand the importance of growth and profitability and our solutions are designed to enhance both. As a consulting firm that can fully implement whatever it recommends, Tevora works with all of the industry's top vendors, yet is beholden to none. We are completely vendor-independent and select best-of-breed products tailored exclusively to our clients' needs. Security is our only business and our single-minded focus on anticipating and solving client problems has been described as "obsessive." We consider this a fair assessment.

Our hard work and dedication have established us as a reliable partner CTOs CIOs, and CISOs can depend on to help protect against threats, both internal and external. With Tevora as a partner, business leaders can devote their energies to enhancing the overall value of information technology to their enterprise.

Tevora is a Qualified Security Assessor (QSA) and Payment Application Qualified Security Assessor (PA-QSA) in good standing with the PCI Security Standards Council. Tevora is also a DVBE (Disabled Veteran Business Enterprise) certified by the California General Services Department (Cert REF# 32786).

For more information, please visit tevora.com.

Our team is ready to discuss your specific challenges and identify the best solutions.

Give us a call at (833) 292-1609 or email us at sales@tevora.com.

TEVORA™

Go forward. **We've got your back.**