ISO 27701 - How OneTrust Helps

AUGUST 2019

WHITE PAPER

OneTrust Privacy
PRIVACY MANAGEMENT SOFTWARE

Table of Contents

DISCLAIMER

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. OneTrust LLC. shall have no liability for any error or damage of any kind resulting from the use of this document.

OneTrust products, content, and materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue. OneTrust materials do not guarantee compliance with applicable laws and regulations.

Introduction

The constantly changing landscape of information privacy and security necessitates guidance on how to operate within this ever-growing sphere. International standards have been established to provide guidance on how organizations should handle personal information and how to demonstrate compliance as privacy regulations continue to evolve.

As the overlap of privacy and security regulations increases, so do the calls for new ways for these two teams to collaborate, communicate more effectively, and use common tools. OneTrust helps with the establishment, maintenance and continual improvement of a privacy information management system (PIMS) in accordance with ISO 27701 (formerly known as "ISO 27552"), as well as the planning and implementation of global privacy laws and frameworks.

What is a PIMS?

A Privacy Information Management System (PIMS) consists of the combination of an Information Security Management System (ISMS) and the more specific requirements for personal data protection. A PIMS is an organization's systematic approach to integrating the protection of privacy with its information security efforts. More specifically, a PIMS includes policies, procedures, guidelines, resources, activities, and controls employed in pursuit of that aim.

One of the overarching goals of a PIMS is to implement Privacy by Design—the proactive embedding of privacy into the design specifications of information technologies, network infrastructure and business practices. Privacy by Design is made less complex by the guidance provided in ISO 27701 on how to establish, implement, maintain, and continually improve a PIMS. An effective PIMS necessitates skilled decision-making, documented policies and procedures, awareness training, clear lines of responsibility and process ownership, privacy impact assessments and treatment plans, data mapping, incident response, vendor management, internal auditing, and more.

What is ISO 27701?

ISO 27701 is a privacy extension to ISO/IEC 27001 that establishes additional requirements and provides guidance for the safeguarding of privacy as potentially affected by personal data processing. These requirements and recommendations facilitate organizations' inclusion of requirements regarding information security and protection of personal data into their general Management System. Specifically, ISO 27701 details what is necessary for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS). ISO 27701 provides practical guidance that can be used by personal data controllers, (including joint personal data controllers) and personal data processors (including those using subcontractors) to manage their privacy program.

ISO 27701 specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) as an extension to ISO 27001 for privacy management within the context of the organization. To comply with ISO 27701, organizations must meet the requirements of ISO 27001, taking into account, in addition to information security, the protection of privacy principals as potentially affected by personal data processing.

Clause 5.1 of ISO 27701 features the PIMS-specific requirements related to ISO 27001. All requirements of ISO 27001 Clauses 4 – 10 that are not included in ISO 27701 apply without any specific revisions.

Generally, ISO 27701 expands information security, and extends the requirements in ISO 27001 mentioning "information security," to include the privacy of information and the protection of privacy as potentially affected by personal data processing.

How OneTrust Helps with ISO 27701

By following the instruction of ISO 27701, organizations of all sizes and industries should be able to document evidence and demonstrate compliance regarding its processing of personal information, and to align or integrate its PIMS with the requirements of other Management System standards. This documentary evidence helps establish transparency, facilitate trust, and promote collaboration. Further, requirements of ISO 27001 and the General Data Protection Regulation ("GDPR") share significant common ground such that implementing ISO 27701 can help organizations work together internally to reduce risk to people and organizations caused by the misuse of personal data.

The following provides an overview of how OneTrust helps with ISO 27701 and privacy information management, relating specifically to:

- PIMS Decision-Making
- Documentation
- Privacy Training, Testing and Attestation
- Internal Audits
- Records of Processing Activities
- Risk Assessment and Treatment
- Vendor Management
- Incident Response
- Data Subject Request Management
- Consent Management

PIMS Decision-Making

ISO 27701 provides a roadmap for building a comprehensive PIMS. This roadmap includes determining both the internal and external issues that might affect privacy (including taking the interests of third parties into account) to determine scope and context, and then creating policies and procedures to match.

Specifically, Clause 5.2 of ISO 27701 requires that you identify where your organization acts as a personal data controller (including joint personal data controller) and a personal data processor. Further, it mandates that you document the internal and external factors affecting your PIMS, as well as the needs and expectations (including requirements) of any interested parties that are relevant to the PIMS, and that you take these things into account when determining the scope (i.e., the boundaries and applicability) of your PIMS. Finally, Clause 5.2 requires that the PIMS be formally documented and undergo continuous improvement.

Clause 5.3 is concerned with leadership and responsibilities—ensuring an organization-wide commitment to privacy, communicating a documented privacy policy throughout the organization, and having defined roles and responsibilities with respect to privacy operations.

Clause 5.4 is about planning—including creating a documented procedure for identifying, assessing and treating privacy risks and opportunities for improvement, as well as a process identifying privacy objectives and creating detailed plans on how to achieve them. Risk treatment plans and PIMS objectives should be "S.M.A.R.T."—Specific, Measurable, Achievable, Relevant, and Time bound. Finally, Clause 5.4 requires you to create a "statement of applicability" that documents the ISO/IEC 27701:2019 Annex A/B controls that have deemed applicable to the ISMS.

Clause 5.5 is about support for the PIMS. It requires that you allocate the resources necessary for achieving your objectives and to ensure continuous improvement of your PIMS, as well as ensuring that in-scope personnel have the necessary levels of privacy education, training and experience. It also requires that you ensure organization-wide awareness of privacy policies and procedures, and individual roles and responsibilities with respect to privacy (e.g., that privacy is the responsibility of all personnel). Lastly, clause 5.5 requires a documented policy and procedure for handling both internal and external communications about the PIMS, as well as a documented policy and procedure for ensuring the proper review and approval of new or updated PIMS documentation, as well as for proper control and handling of documentation.

Clause 5.6 is primarily about implementation of the plans set out in Clause 5.4. It requires that you undergo risk assessments at planned intervals or when significant changes are planned or occur, and that you document the results. It subsequently requires you to create and carry out risk treatment plans following the risk assessment, and to document the results of treatment.

Clause 5.7 requires that you conduct internal audits of the PIMS against the ISO/IEC 27701:2019 standard (including all of clause 5 and applicable Annex A/B controls), and that you conduct management reviews of the PIMS at planned intervals.

Lastly, Clause 5.8 calls for a documented corrective action procedure for addressing 'nonconformities' with the ISO/IEC 27701:2019 standard. Nonconformities are typically identified during audits. Nonconformities identified during an external certification or surveillance audit are typically accompanied by deadlines for completing corrective actions, and in some cases a failure to correct a nonconformity can result in loss of certification.

Use the ISO 27701 PIMS Planning template in OneTrust to assist with PIMS decision-making according to clause 5 of the ISO 27701 standard, including evaluating your organization and its context, understanding the needs and expectations of interested parties, determining the scope of the PIMS, identifying leadership roles and responsibilities, establishing and tracking objectives, defining risk criteria, and more.

Documentation

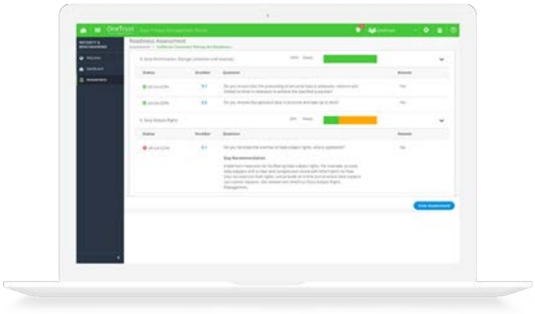
ISO 27701 requires a substantial amount of documentation to be created, reviewed, updated and properly controlled over the life of the PIMS. This documentation is vital to the effectiveness and continuous improvement of the PIMS, as well as to achieving and maintaining certification.

A common approach to storing documentation is to organize it according to the structure of the ISO/IEC 27701:2019 standard—e.g., a folder containing core documents that address clause 5 of the standard, a folder containing policies and procedures specifically addressing applicable Annex A/B controls, a folder containing frequently used template documents (e.g., template agreements, training slides, etc.), and a folder containing evidence of security operations and implementation.

Use the Document Repository in OneTrust to store and organize PIMS documentation in a central location for access by the PIMS Team and other need-to-know personnel.

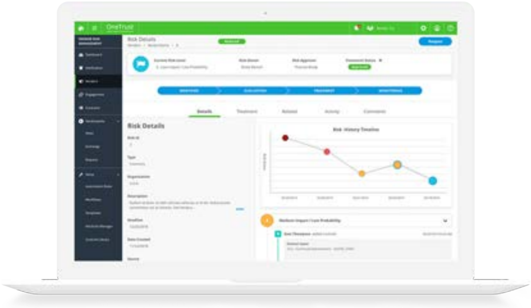
Privacy Training, Testing and Attestation

Clause 5.5 requires that employees and contractors be made aware of the organization's privacy policy, their individual contributions, roles and responsibilities in the PIMS, and the consequences of not conforming to requirements. Additionally, Annex A/B requires that all employees and contractors receive information privacy awareness education and training, as well as regular updates on applicable policies and procedures.



OneTrust training templates, such as the "Privacy and Security Training Quiz and Attestation" template, can be used to assist with testing the effectiveness of awareness training, as well as to record employee attestations to acceptable use policies or employee responsibility documents.

Risk Assessment and Treatment

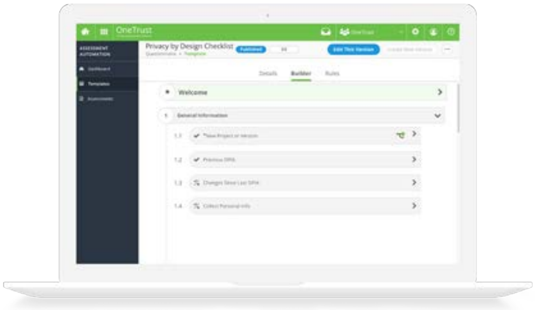


Clause 5.4 requires the creation of a detailed risk assessment methodology that includes criteria for how to identify different levels of risk (i.e., what constitutes high versus low impact to the individual or organization, and what types of risk can be accepted without additional treatment), a procedure for creating and carrying out risk treatment plans, the frequency of risk assessments, and more.

Clause 5.6 then requires the implementation of these plans—i.e., following the risk methodology when conducting risk assessments, setting risk treatment plans and tracking them to completion, calculating residual risk, and ensuring that all of this is documented in a controlled manner. During the risk assessment process, organizations should manage the relationship between privacy and security appropriately, either using an integrated privacy and information security risk assessment process or two separate processes.

Use OneTrust Assessment Automation, and an extensive gallery of questionnaire templates, to identify and calculate risks to individuals as a result of processing their personal information, and to craft and track risk treatment plans.

Internal Audits

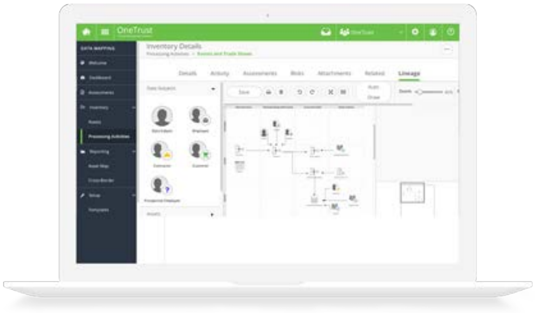


Clause 5.7 requires that you conduct internal audits of the ISMS against the ISO/IEC 27701:2019 standard (including all of clause 5 and applicable Annex A/B controls). Moreover, Clause 5.7.3 calls for management reviews of the PIMS at planned intervals.

Use the "**ISO 27701 Audit Checklist**" **template**, a fully customizable questionnaire in OneTrust based on ISO 27701 to assist in conducting internal or external audits of the PIMS, to evaluate the maturity and overall effectiveness of the PIMS, and to track corrective action plans. After completing an audit, OneTrust allows you to easily generate an audit report showing an overview of your answers, comments and evidence attachments.

OneTrust is also great for documenting and demonstrating the continual improvement of an ISMS. With assessment versioning and reporting features, you can easily see how your program has grown year over year.

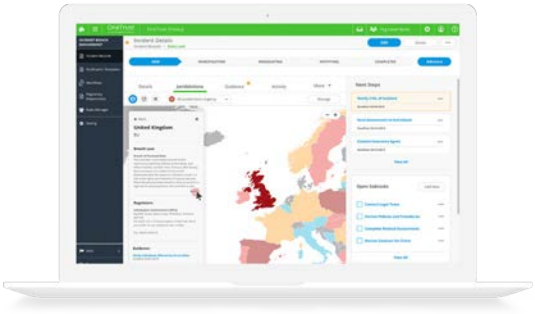
Records of Processing



Annexes A.7.2.8 and B.8.2.6 recommend organizations establish what records are necessary in support of its processing obligations and maintain/preserve them. Organizations should create and maintain an inventory or detailed list of all the personal data processing activities it executes, which includes details such as the type and purpose of the processing, and any other details considered necessary and pertinent. The inventory should have an assigned owner who has the duty of ensuring its correctness and totality. Additionally, some jurisdictions have specific recordkeeping requirements that may include a Privacy Impact Assessment report or the categories of recipients, including those in third countries or international organizations, who have or will be receiving personal data.

With OneTrust you can create and maintain inventories of your organization’s assets and vendors, the risks associated with each, and their owners within the organization. Additionally, OneTrust automatically generates visualizations and data flow diagrams as tools for easier analysis and executive communication. OneTrust provides multiple ways for you to map data flows across your organization. Our built-in questionnaire template can be easily tailored and helps collect information about the purpose, type and process by which personal data is being collected, used, stored, and transferred.

Incident Response



Clause 6.13.1.1 states that an organization’s incident management process should feature the responsibilities and processes related to identifying and recording breaches of personal data processing. Further, applicable requirements and obligations regarding breach notification should be determined. Many jurisdictions feature and impose their own requirements related to breach response and notification, and organizations’ compliance across these many jurisdictions is vital.

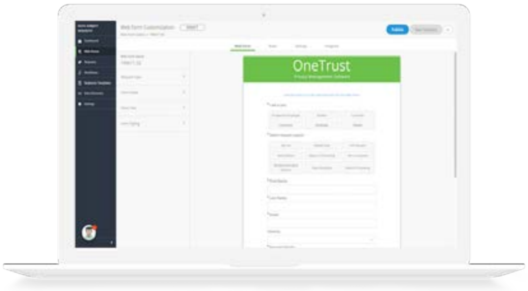
With OneTrust, you can enable self-service reporting of security incidents and weaknesses, maintain incident and breach records, evaluate against breach notification obligations, and analyze overall risk with connections to your underlying inventories of data, processing activities, assets and vendors. OneTrust can be used to put incident management policies and procedures into action.

Consent

Annexes A.7.2 and A.8.2 feature requirements for personal data controllers and processors and state that processing must be lawful, based on legitimate purposes or consent, and/or jurisdiction specific lawful bases of processing. Under ISO 27701, consent must be obtained, where applicable, from Individuals and recorded so that details, such as when consent was provided, proof of identity of the Individual, and the consent statement, can be provided on request.

Use OneTrust Consent Management tool to demonstrate compliance with granular records of consent. OneTrust provides the platform and instruments necessary to collect valid consent as required by ISO 27701, as well as privacy regulations such as GDPR, CCPA, and LGPD. Additionally, the OneTrust Cookie Consent tool facilitates the collection of valid consent by informing website visitors about a company's cookies and tracking technologies in use on their websites, as well as providing users with granular choice and control over their consent.

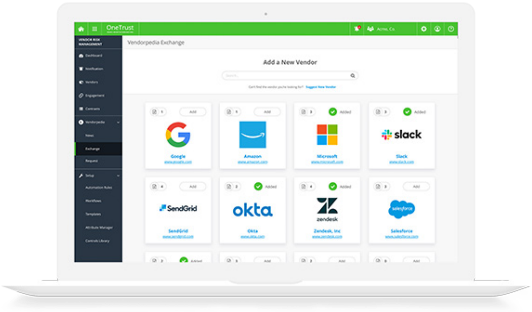
Data Subject Request Management



Annex A.7.3 details a personal data controller's obligations to Individuals. Individuals should be provided with the proper information about the processing of their personal data, as well as any other relevant obligations related to its processing. An organization should establish, document, and uphold their obligations to Individuals as demanded by legal and business requirements. Obligations to Individuals should be met in an accessible, timely, and transparent manner, with clear documentation provided to Individuals detailing how the obligations are satisfied and contact information to address their requests.

OneTrust provides a standardized way for privacy programs to receive requests and manage them in a centralized system. OneTrust provides organizations with the ability to tailor a branded web form – linked from your company's privacy policy web page – as well as the ability to receive notification of a submitted request, validate the identity, and automatically file an extension if a deadline is approaching. When the request is fulfilled, the organization must securely transmit the data to the individual, link it to the underlying data map to efficiently fulfill the request, and generate the proper documentation and evidence should a regulator inquire about the request.

Vendor Management



Clauses 6.12, 7.2.6, and 7.5 feature guidance on supplier relationships, contracts with processors, and the requirements for personal data sharing, transfer, and disclosure. According to clause 6.12.1.2, organizations should include specific terms in contracts between themselves and any subcontractor on whether personal data is being processed and the necessary technical and organizational protocols which satisfy the organizations information security and personal data protection requirements.

Clause 7.2.6 states that contracts between the organization and any personal data processor should require implementation of the appropriate Annex B controls with respect to the information security risk assessment process and the extent of the processor's personal data processing. The justification for the exclusion of any Annex B controls should be documented as they are all relevant by default.

Lastly, clause 7.5 recommends that organizations determine and document the applicable basis for international transfers of personal data based on the relevant law, jurisdiction, or the international organization which is receiving or originating the data to be transferred. Records of transfer and disclosure of personal data to or from third parties should be maintained, with a defined policy on how long the records are kept.

Use OneTrust Vendorpedia, third-party risk and vendor management software, to gain insight into the security and privacy risks of third parties at a granular level, including the vendor risks in general, and risks specific to engagements, products or services, contracts, processes or IT systems. With OneTrust, your organization can automate the vendor engagement lifecycle, from onboarding to offboarding, with free vendor chasing services and automated workflows to manage IT and non-IT vendors, direct suppliers, services and legal organizations, franchisees and retailers, as well as agents and contractors. The OneTrust platform allows your organization to assess vendors with greater flexibility to fit your use case, with support for every industry standard, framework, and law, including CSA CAIQ, SIG, SIG Lite, HITRUST, PCI DSS, NIST, ISO 27001, GDPR, NYDFS, CCPA, and many more. Additionally, OneTrust provides access to aggregated vendor information without having to scour the web. OneTrust Vendorpedia does the research for you, prepopulating privacy and security data on thousands of global vendors, each with information at the service-and product-level.

Conclusion

Ultimately, ISO 27701 implementation gives organizations the opportunity to bolster and expand their existing ISMS by extending the requirements of ISO 27001 to the privacy of information and protection of privacy as potentially affected by personal data processing. This extension of ISO 27001 also leads to internal collaboration as the privacy and information security teams work together to implement the requirements of ISO 27701 while maintaining distinct roles and responsibilities.

About OneTrust

OneTrust is the #1 most widely used privacy, security and third-party risk technology platform trusted by more than 3,000 companies to comply with the CCPA, GDPR, ISO 27001, ISO 27701 and hundreds of the world's privacy and security laws. OneTrust's three primary offerings include OneTrust Privacy Management Software, OneTrust PreferenceChoice™ consent and preference management software and OneTrust Vendorpedia™ third-party risk management software and vendor risk exchange.

OneTrust products can be used standalone – or seamlessly integrate together – to give you the right-sized technology for your privacy, security and third-party risk programs. Powered by an intelligence database of hundreds of laws, OneTrust adapts to the jurisdictions and frameworks that matter most to you, generating the right dashboards, visuals and record keeping reports you need.

OneTrust is co-headquartered in Atlanta and in London, and has additional offices in Bangalore, San Francisco, Melbourne, New York, Munich and Hong Kong. Our fast-growing team of privacy, security and third-party risk technology experts surpasses 1,000 employees worldwide.

Backed and co-chaired by the founders of Manhattan Associates (NASDAQ: MANH) and AirWatch ($1.54B acq. by VMware), and supported by a $200 million Series A funding from Insight Partners, the OneTrust leadership team has significant experience building scalable, enterprise software platforms.

To learn more, visit **onetrust.com**.

OneTrust Privacy

PRIVACY MANAGEMENT SOFTWARE

ONETRUST.COM

ATLANTA | BANGALORE | HONG KONG | LONDON
MELBOURNE | MUNICH | NEW YORK | SAN FRANCISCO