ISO 27701
PRIVACY INFORMATION MANGEMENT SYSTEMS

DEKRA

ISO 27701 is a privacy-focused standard for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS) as an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization. ISO 27701 was created by ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) in a way that it incorporates articles from the EU General Data Protection Regulation (GDPR) and other ISO frameworks.

Defining Data Privacy

Data privacy involves the protection of Personally Identifiable Information (PII) during the collection, usage, and sharing of that data. Personally Identifiable Information can include any information that has the potential to be used to identify someone, such as names, social security numbers, addresses, and phone numbers, and more. Today we are more connected than ever, with internet usage jumping to a whopping 4.5 billion internet users globally as of mid-2019[1], so the number of people whose information is stored digitally is growing quickly.

There is global concern regarding data privacy; in the United States, 82% surveyed said they worried about their data privacy and online security[2]. And they may have reason to: 15% of companies using the internet to conduct business do not yet use Secure Socket Layer (SSL) encryption. In 2018, in the U.S. alone, 1.244 billion data breaches occured, exposing over 446 million records[3].

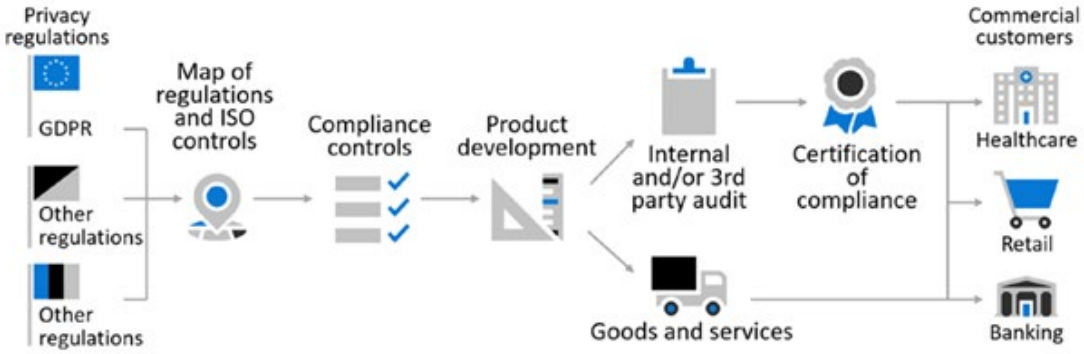
The Importance of ISO 27701

Almost every organization processes Personally Identifiable Information, whether belonging to their clients or employees. As organizations grow, expand, and adopt new technologies, the quantity and variety of the PII processed increases, as does the number of information security laws and regulations in force around the world.

Benefits of ISO 27701

- Ensures compliance with privacy laws and regulations governing PII for controllers and processors
- Globally recognized and respected standard that is mapped to GDPR, UK DPA, HIPPA, and CCPA requirements, as well as to other ISO standards
- Provides practical, clear measures on how to safeguard PII
- Builds trust and privacy awareness
- Provides transparency between stakeholders

1 https://www.internetworldstats.com/stats.htm
2 https://www.vpngeeks.com/internet-privacy-statistics/
3 https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/



Compliance Challenges

ISO 27701 addresses three key compliance challenges:

> Too many regulatory requirements to juggle
Reconciling multiple regulatory requirements through the use a universal set of operational controls enables consistent and efficient implementation.

> Too costly to audit regulation-by regulation
Auditors, both internal and third party, can assess regulatory compliance using a universal operational control set within a single audit cycle.

> Promises of compliance without proof is potentially risky
Commercial agreements involving movement of personal information may warrant certification of compliance.[4]

Defined Roles in Privacy Management

The roles specified in the ISO 27701 standard include controllers and processors, which are defined in Article 4 of the GDPR.

A **controller** is a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."

A **processor** is a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[5]

Structure of ISO 27701

ISO 27701 can be divided into privacy-centric clauses (5-8) and annexes (A-F). According to the official documention, Clause 5 gives PIMS-specific requirements and other information regarding the information security requirements found in ISO/IEC 27001 that are appropriate to an organization acting as either a PII controller or a PII processor.

Clause 6 gives PIMS-specific guidance and other information regarding the information security controls in ISO/IEC 27002 and PIMS-specific guidance for an organization acting as either a PII controller or a PII processor.

Clause 7 gives additional ISO/IEC 27002 requirements for PII controllers, and Clause 8 gives additional ISO/IEC 27002 requirements for PII processors.

This structure also includes six important annexes that provide implementation guidance for the standard.

Annex A (PII Controllers)

This annex is used by organizations acting as PII controllers, with or without the use of PII processors. It acts as an extension of ISO/IEC 27001:2013, Annex A.

Annex B (PII Processors)

This annex is used by organizations acting as PII processors, with or without the use of PII subcontractors. It acts as an extension of ISO/IEC 27001:2013, Annex A.

Annex C (Mapping to ISO 29100)

This annex maps privacy principles that are related to provisions of ISO 27701, including those relevant for controllers and those relevant for processors.

Annex D (Mapping to GDPR)

This annex gives an indicative mapping between provisions of this document and Articles 5 to 49, except 43 of the General Data Protection Regulation of the European Union. It shows how compliance to requirements and controls of this document can be relevant to fulfill obligations of GDPR. However, it is purely indicative, and as per official ISO 27701 document, it is ultimately the organization's responsibility to assess its legal obligations and decide how to comply with them

Annex E (Mapping to ISO 27018 & 29151)

ISO/IEC 27018 gives further information for organizations acting as PII processors and providing public cloud services. ISO/IEC 29151 offers additional controls and guidance for the processing of PII by PII controllers. The ISO 27701 official documentation provides an indicative mapping between provisions of this document and provisions from ISO/IEC 27018 and ISO/IEC 29151. It shows how requirements and controls of this document can have some correspondence with provisions from ISO/IEC 27018 and/or

4 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3uDwE
5 https://ec.europa.eu/info/law/law-topic/data-protection_en

Keeping Proper Records of Breaches

WHERE A BREACH INVOLVING PII HAS OCCURRED, A RECORD SHOULD BE MAINTAINED WITH SUFFICIENT INFORMATION TO PROVIDE A REPORT FOR REGULATORY AND/OR FORENSIC PURPOSES, INCLUDING:

- a description of the incident;
- the time period;
- the consequences of the incident;
- the name of the reporter;
- to whom the incident was reported;
- the steps taken to resolve the incident (including the person in charge and the data recovered);
- whether the incident resulted in unavailability, loss, disclosure or alteration of PII.

ISO/IEC 29151. It is purely indicative, and one should not assume that a given link between provisions means exact equivalence.

Annex F (Mapping to ISO 27001 & 27002)

Annex F shows how auditors can implement the ISO 27701 standard by mapping it with ISO 27001 and ISO 27002. It extends their requirements and guidance to take into account, in addition to information security, the principles of protection of privacy as potentially affected by the processing of PII. That means that where the term "information security" is used in ISO 27001 or ISO 27002, "information security and privacy" can apply as well.

Implementation Guidance for PII Controllers

An incident that involves PII should trigger a review by the organization, as part of its information security incident management process, to determine if a breach involving PII that requires a response has taken place. An event does not necessarily trigger such a review.

An information security event does not necessarily result in actual, or the significant probability of, unauthorized access to PII or to any of the organization's equipment or facilities storing PII. These can include, but are not limited to, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks and packet sniffing.

When a breach of PII has occurred, response procedures should include relevant notifications and records. Some jurisdictions define cases when the breach should be notified to the supervisory authority, and when it should be notified to PII principals. Notifications should be clear and can contain details, such as a contact point where more information can be obtained, a description of the the breach including the number of individuals and/or records concerned, likely consequences of the breach, and measures taken or planned to be taken.

Implementation Guidance for PII Processors

Provisions covering the notification of a breach involving PII should form part of the contract between the organization and the customer. The contract should specify how the organization will provide the information necessary for the customer to fulfil their obligation to notify relevant authorities. This notification obligation does not extend to a breach caused by the customer or PII principal or within system components for which they are responsible, as well as expected and externally mandated limits for notification response times.

In some jurisdictions, the PII processor should notify the PII controller of the existence of a breach without undue delay (i.e. as soon as possible) - preferably, as soon as it is discovered so that the PII controller can take appropriate actions

DEKRA Can Help

Here at DEKRA we protect people, assets, and our community by providing a comprehensive testing, inspection, certification, and consulting services around the globe. We are the world's leading Safety Solutions provider with more than 44,000 employees and around €3.1 billion in revenues worldwide.

In this rapidly changing digital economy, nearly every company is in the business of data. If your organization is already ISO 27001 certified, then most of the work has already been done for your ISO 27701 certification, because privacy goes hand-in-hand with security. Our certified auditors can take steps to ensure the privacy of your Personally Identifiable Information, such as:

> **Security and privacy gap assessments between your existing systems and the requirements of ISO 27001 and ISO 27701**
> **PII processing assessments to examine the scope of PII collected, processed, and shared**
> **Regulatory assessment to determine the role of the organization as controller or processor in the eyes of local privacy regulations**
> **Documentation of privacy decision-making processes**