PECB

Whitepaper

THE FUTURE OF PRIVACY WITH ISO/IEC 27701

Table of contents

Introduction 03

What is ISO/IEC 27701? 04

PII controller and processor 05

The structure of ISO/IEC 27701 05

Why ISO/IEC 27701? 08

The relationship between ISO/IEC 27701 and other ISO standards 09

The relationship between ISO/IEC 27701 and GDPR 10

Conclusion 11

Training course and certification 11

PRINCIPAL AUTHORS

- Eric LACHAPELLE, PECB
- Faton ALIU, PECB
- Gresa MJEKU, PECB
- Erigon KASTRATI, PECB

CONTRIBUTORS

- Argita Canhasi, PECB
- Enis Shala, PECB
- Artan Mustafa, PECB
- Jetë Spahiu, PECB
- Friedhelm Düsterhöft, msdd.neT GmbH
- Romain Hennion, Deloitte
- Adam Gałach, Galach Consulting Group
- Adrian Horodniceanu, A.H Training @ Technology Ltd.
- Thomas Lionel Smets, net-security-training.eu
- Jeroen Van Der Vlies, Checksec
- Juan Carlos García, Consultit OÜ
- Roy Biakpara, Cryptv Ltd
- Walter Rocchi, Consulthink S.p.A.
- David Blampain, david-blampain.com
- Jarek Sordyl, PERN Group - Oil TSO
- Badis Hafhouf, Lineon

Introduction

Organizations planning to expand their operations, activities, and processes in the future will have to depend on digital transformation to ensure their existence. The old industrial age of manufacturing is being replaced at a rapid pace by the new information age where knowledge creation, service delivery, and the value of information have dramatically developed. This development that is presently stimulated by the advent of cheap internet connectivity, easy access to information, and low storage costs has accelerated this digital transformation. On the other hand, technology advancements such as Internet of Things (IoT) devices have become more affordable to users.

Information is highly sought after and this depends mainly on the intrinsic value that the information possesses. Organizations can make highly personalized products and services to their clients through successful market advertisements that are targeted directly towards their interests. However, organizations that use client data can sometimes be vulnerable to cybercriminals and other threat sources that frequently target these organizations to extract personally identifiable information. If successful, the cybercriminals and other threat sources use organizations' client data for reasons that, among others, include identity theft and financial fraud; a phenomenon that is proving to be difficult to manage. Therefore, information becomes a prime target for the misuse of a lot of entities but also makes services and products highly customizable to the specific needs of each customer, making it a challenge to reach a balance between good products or services and privacy.

Privacy is (or has been recently emphasized as) a necessity for a rather open society in the modern computer age. Accordingly, measures are being taken and this is being reflected by the implementation of dedicated laws and regulations all over the world.
Non-profit organizations such as NOYB (None Of Your Business) are continuously pointing out flaws in legislation that allow organizations to escape accountability regarding their processing of Personally Identifiable Information (PII) and compliance to the General Data Protection Regulation (GDPR).

Privacy does not mean secrecy. A private matter is something that someone does not want to share with the whole world; conversely, a secret matter is something that someone does not want anyone else to know. Privacy is rather the ability and also the power to reveal oneself to the world by choice and will. In an open society, the use of strong cryptography, such as Pretty Good Privacy (PGP), pseudonymization, data anonymization, and other technical and organizational measures safeguard the individuals' privacy.

There are several compelling reasons that lead to the development and enactment of GDPR and other data privacy laws. Many studies have claimed that the mere fact of knowing that people are observed in social media may change their behavior, let alone knowing that there is an authority observing every move they make. Thus, decisions made in this manner are not the by-product of a person's own agency but the expectations that others have of them. This leads users to display behavior that is vastly more conformist and compliant, thus severely reducing the range of behavior options.

Considering that GDPR is a regulation on data protection and privacy for all individuals that reside in the European Union (EU) and the European Economic Area (EEA), countries outside the EU and EEA have started to create their own data protection laws. As a response to this market need, the International Organization for Standardization (ISO), an international organization of worldwide recognition and the oldest and most experienced in the field of industry standardizations, in cooperation with the International Electrotechnical

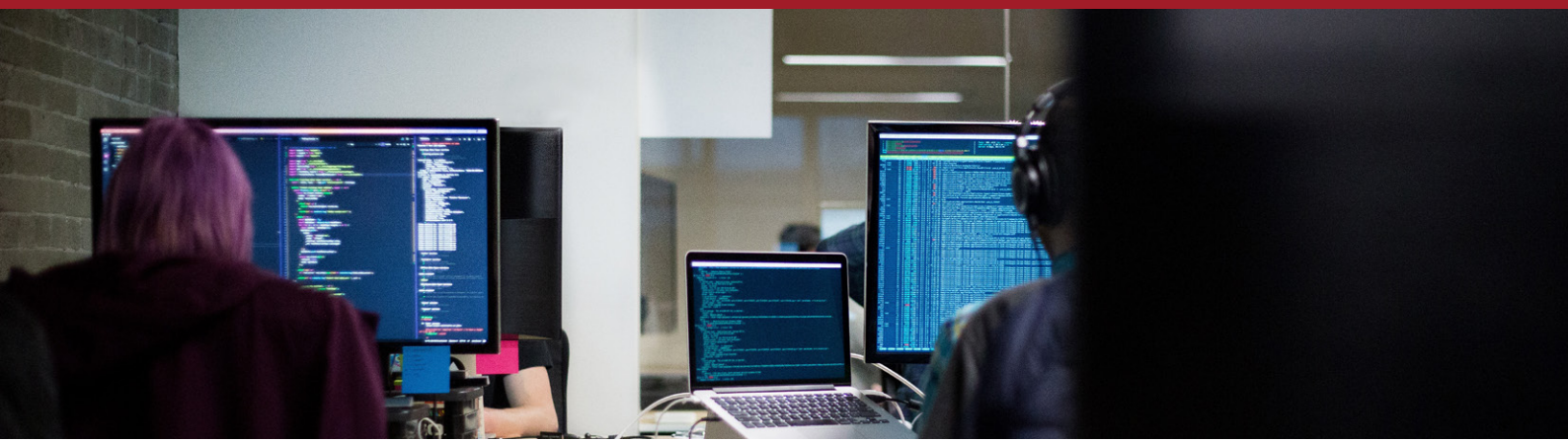
Commission (IEC), have decided to prepare standards that provide privacy guidance applicable to any organization regardless of the size, type, or country where they operate. Their newest standard that is being developed on this matter is ISO/IEC 27701 — *Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines*.

What is ISO/IEC 27701?

ISO/IEC 27701 specifies requirements and provides guidance for establishing, maintaining, and continually improving a Privacy Information Management System (PIMS) as an extension to the ISMS implementation based on the requirements of ISO/IEC 27001 and the guidance of ISO/IEC 27002.

This standard can be used by PII controllers and PII processors. The additional requirements and guidance for PII protection are applicable to any organization and can be adopted regardless of the size and cultural environment of the organization.

ISO/IEC 27701 provides information on mapping this standard to the privacy framework and principles defined in ISO/IEC 29100. Furthermore, it also includes mapping to ISO/IEC 27018, ISO/IEC 29151 and GDPR.



PII controller and processor

ISO/IEC 27701 is designed to be used by all PII controllers, including joint PII controllers, and all PII processors including subcontracted PII processors and subcontractors to PII processors.

In the ISO/IEC 29100 standard, personally identifiable information PII is defined as "any information that can be used to identify the PII principal to whom such information relates, or is or might be directly or indirectly linked to a PII principal." A PII controller is defined as a "privacy stakeholder that determines the purpose and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes." A PII controller defines the "why" and "how" the PII processing will be performed. In addition, it is their responsibility to implement privacy and security controls based on the relevant jurisdictions.

When there is more than one PII controller, they shall work together to ensure privacy principles are followed during the PII processing and this is known as a joint PII controller. Joint PII controllers are mutually held liable by the GDPR.

The ISO/IEC 29100 standard defines a PII processor as a "privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller." A PII processor acts based on the PII controller's instructions and implements the privacy controls. The PII processor is usually subject to fewer legal obligations compared to the PII controller because the responsibility for the processing remains within the PII controller. However, GDPR defines strict requirements regarding the relations between the controller and the processor, as stated in Article 28. The PII processor is usually a third party external to the company. For example, cloud computing providers are normally PII processors, as are external companies who gain access to IT systems for maintenance purposes.

The duties that the PII processor has towards the controller must be specified prior to the handling of the PII in a contract or other legal act. The contract must indicate what happens to the PII once the contract terminates. Nonetheless, there are cases where one entity besides being a PII controller can also be a PII processor.

The structure of ISO/IEC 27701

ISO/IEC 27701 is an extension of ISO/IEC 27001 and ISO/IEC 27002. It extends the ISO/IEC 27001:2013 requirements and ISO/IEC 27002:2013 guidelines by providing additional PIMS-specific requirements (see Table 1). Sinc e its prime objective is to enhance the existing ISMS, the term "information security" is substituted with the term "information security and privacy."

Table 1: ISO/IEC DIS 27701 clauses

Clause number and title	Sub-clauses
Clause 5 PIMS-specific requirements related to ISO/IEC 27001	**5.1 General** The requirements of ISO/IEC 27001:2013 mentioning "information security" shall be extended to the protection of privacy as potentially affected by the processing of PII.
	5.2 Context of the organization 5.3 Leadership 5.4 Planning 5.5 Support 5.6 Operation 5.7 Performance evaluation 5.8 Improvement
Clause 6 PIMS-specific guidance related to ISO/IEC 27002	**6.1 General** The guidelines in ISO/IEC 27002:2013 mentioning "information security" should be extended to the protection of privacy as potentially affected by the processing of PII.
	6.2 Information security policies **6.3** Organization of information security **6.4** Human resource security **6.5** Asset management **6.6** Access control **6.7** Cryptography **6.8** Physical and environmental security **6.9** Operations security **6.10** Communications security **6.11** Systems acquisition, development and maintenance **6.12** Supplier relationships **6.13** Information security incident management **6.14** Information security aspects of business continuity management **6.15** Compliance
Clause 7 Additional ISO/IEC 27002 guidance for PII controllers	**7.1 General** The guidance contained in Clause 6 plus the additions in the current clause create the PIMS-specific guidance for PII controllers. The implementation guidance documented in the current clause relate to the controls listed in Annex A.
	7.2 Conditions for collection and processing **7.3** Obligations to PII principals **7.4** Privacy by design and privacy by default **7.5** PII sharing, transfer, and disclosure
Clause 8 Additional ISO/IEC 27002 guidance for PII processors	**8.1 General** The guidance contained in ISO/IEC 27002:2013 plus the additions of this clause create the PIMS-specific guidance for PII processors. The implementation guidance documented in clause 8 relate to the controls listed in Annex B.
	8.2 Conditions for collection and processing **8.3** Obligations to PII principals **8.4** Privacy by design and privacy by default **8.5** PII sharing, transfer and disclosure

Clause 5 presents the PIMS-specific requirements related to ISO/IEC 27001, which are appropriate for an organization acting as either a PII controller or a PII processor. The requirements of clause 5 are mandatory; meaning that the organization cannot otherwise claim conformity to ISO/IEC 27701.

Nevertheless, there may be cases when some of the controls that are presented in Annex A and B are not applicable to an organization because of its unique nature. As a result, they may be excluded in the PIMS implementation. Similar to ISO/IEC 27001, a justification for excluding the implementation of any control shall be included in the Statement of Applicability.

Clause 6 presents the PIMS-specific guidance related to information security controls in ISO/IEC 27002, which again are appropriate for an organization acting as either a PII controller or a PII processor.

Clause 7 presents the PIMS-specific guidance for PII controllers, while clause 8 of this standard presents the PIMS-specific guidance for PII processors. Both are organized and structured similarly.

Annexes A and B of this standard provide information and guidance regarding PIMS-specific reference control objectives and controls for PII controllers and processors. Annexes C, D, and E provide information and guidance with regard to mapping this standard against GDPR and other ISO/IEC standards. Annex F illustrates the terms used in this standard and the alternative terms used in specific jurisdictions, while Annex G presents guidance on how to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002 requirements and guidance.

Why ISO/IEC 27701?

Personal information is everywhere and it is growing exponentially. Information is being collected, processed, stored, and transmitted in many forms within all types of organizations on a daily basis.

Organizations engaged in this process experience a competitive atmosphere and should be aware of the need to acknowledge and accept the responsibilities and be held accountable for the effective handling of PII. Therefore, one of the main reasons why organizations should seek an ISO/IEC 27701 certification is to comply with GDPR and encounter fewer costs when it comes to customer and supplier audits.

ISO/IEC 27701 provides information on how organizations should manage and process data to protect privacy and personally identifiable information. This standard improves the ISMS and it helps addressing PIMS accurately. The framework of this draft standard serves as a guideline towards the establishment, implementation, maintenance, and improvement of a Privacy Information Management System. It helps organizations understand the practical approaches that are involved in the implementation of an effective management of PII. Therefore, being in conformity to ISO/IEC 27701 may enable your organization to assess, treat, and reduce risks to personal information.

Considering the advantages of implementing an ISMS and the increased need for privacy during the recent years, the implementation of a PIMS based on ISO/IEC 27701 is supposed to offer a competitive advantage in the business market and improve organizations' reputation. In addition, it may also affect customer satisfaction and increase the level of client trust towards the organization. Being certified against ISO/IEC 27701 may make clients feel confident and secure that their personally identifiable information is safe and used for the primary purpose it was collected in the first place. This may increase the transparency of the organization's processes and procedures, thus maintaining integrity to customers and the organization's interested parties.

The relationship between ISO/IEC 27701 and other ISO standards

The ISO/IEC 27000 family of standards is dedicated to information security. There are three requirement standards, ISO/IEC 27001 *Information security management systems — Requirements, ISO/IEC 27006 Requirements for bodies providing audit and certification of information security management systems*, and ISO/IEC 27009 *Sector-specific application of ISO/IEC 27001 — Requirements*. In this list, ISO/IEC 27001 is the only one against which an organization can obtain certification. All other standards are guideline standards such as ISO/IEC 27002 *Code of practice for information security controls*, ISO/IEC *27005 Information security risk management*, or ISO/IEC 27032 *Guidelines for cybersecurity*. Likewise, organizations endeavoring ISO/IEC 27701 certifications will also need to be ISO/IEC 27001 certified.

ISO/IEC 29100 provides a privacy framework applicable to any system or service that requires PII processing. The general privacy principles of this standard are related to the controls of PII controllers and processors, and this mapping is illustrated in Annex D of the ISO/IEC 27701 standard.

ISO/IEC 27018 is based on ISO/IEC 27002 and gives guidance for the protection of PII in public clouds acting as PII processors. Its guidelines are appropriate to organizations acting as PII controllers. ISO/IEC 29151 specifies guidelines based on ISO/IEC 27002, with regards to PII processing requirements. This standard is applicable to organizations acting as PII controllers.

Annex E illustrates ISO/IEC 27701 mapping to these standards; however, this link does not mean equivalence.

The relationship between ISO/IEC 27701 and GDPR

More than twenty years ago, the European Union decided that it is best to align data protection standards within their Member States in order to facilitate EU-internal, cross-border, data transfers. For this purpose, in 1995, the EU adopted the Data Protection Directive.

However, due to the rapid technological advancements, globalization, and failure to prevent fragmentation in the implementation of data protection across the EU, the Data Protection Directive failed to live up to its expectations. Thus, the EU decided to adopt GDPR, whose purpose is best described in the following sentence as stated in Recital 2 of the regulation itself:
"This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons."

Through GDPR, the EU aims to regain people's trust when it comes to the handling of their personal data and boost the digital economy across the EU-internal market.

GDPR is divided into two broad parts: recitals and articles. The articles set out the specific requirements upon which the entities within the scope of the regulation have to comply with. Articles 5 to 49 (with the exception of Article 43) are all related to ISO/IEC 27701 requirements, as illustrated in Annex C of the standard. Article 43, Certification bodies of the GDPR, is excluded from the related ISO/IEC 27701 requirements because it is solely for the accreditation of certification bodies in accordance with GDPR.

Complying with a control requirement of the ISO/IEC 27701 standard serves as evidence that a requirement of GDPR is fulfilled. There are cases where multiple controls cover a specific requirement and others where several GDPR requirements are covered by one control. An example is the mapping of 6.13.1.1 and 6.13.1.5 controls of ISO/IEC 27701 with Article 33 of GDPR. These controls provide guidance on the management of information security incidents, whereas Article 33 presents requirements on the notification of a personal data breach to the supervisory authority.

These two are linked by all measures, excluding the time frame required to notify the data subjects and the privacy regulators which, as required by law, is a period of 72 hours. This example shows that complying with the ISO/IEC 27701 standard will simultaneously assist the organization to demonstrate compliance with GDPR requirements. In general, the standard does not give specific details about the measures that should be taken to comply with control objectives and controls, leaving the decision to the implementer.

In addition, both the GDPR and the draft version of ISO/IEC 27701 use different terminology. GDPR uses the term "personal data," while ISO/IEC 27701 uses the term "Personally Identifiable Information (PII)." Furthermore, GDPR's term "data subject" is replaced with the term "PII principal" in ISO/IEC 27701. Correspondingly, GDPR's terms "data controller" and "data processor" are replaced with the terms "PII controller" and "PII processor" in ISO/IEC 27701.

Conclusion

Having well-established norms regarding privacy will give people confidence towards expressing their opinions, imagination, and dissent in an unbiased manner, regardless of societal influences. A society that is constantly monitored is a society where the freedom of speech and thought is fundamentally compromised.
"All human beings have three lives: public, private, and secret." Gabriel García Márquez

The protection of personally identifiable information is a fundamental human right. The processing of personal data has grown along with the globalization and personalization of services. Consequently, guidelines for security techniques regarding the management of personally identifiable information were necessary.

ISO/IEC 27701 is a sector-specific standard related to ISO/IEC 27001 and ISO/IEC 27002. Compliance against this standard requires evidence on the processing of PII. Moreover, these requirements are independent of the organization's size and cultural environment. Organizations certified against ISO/IEC 27701 will have an easier way of demonstrating compliance with GDPR thus indirectly contributing to a future where privacy is recognized as a human right within the digital realm.

Training course and certification

PECB will be creating a training guide to the personnel certification schemes against the upcoming ISO/IEC 27701 standard. The certification of individuals does not only serve as evidence of professional competency but also that the individual has attended the training course and successfully completed the certification exam. The certificate also validates that the certified professional is equipped with the skills to navigate the regulations and standards specific to privacy and data protection under the information security portfolio.

PECB training courses are offered globally through a network of authorized training providers; they are available in several languages and include the following training courses: Introduction, Foundation, Lead implementer, and Lead Auditor. Knowing that ISO/IEC 27701 is an extension of ISO/IEC 27001 and ISO/IEC 27002, it is worth mentioning that PECB has already created certification schemes for ISO/IEC 27001 and ISO/IEC 27002. ISO/IEC 27001 training courses provide information on how to establish, implement, manage, maintain, and audit an Information Security Management System (ISMS) as well as ISO/IEC 27002 training courses on how to implement information security controls and information security management practices.

Although a specified set of training courses or curriculum of study is not required as part of the certification process, the completion of a recognized PECB training course or program of study will significantly enhance the chances of passing a PECB certification exam as it is based on the PECB's training course material.

The list of approved organizations that offer PECB official training sessions can be found on our website: www.pecb.com.