27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

What is EU GDPR and how can ISO 27001 help?

WHITE PAPER

Advisera
Making certification simple.

Table of Contents

Executive summary

This document examines the EU GDPR and establishes an alignment with ISO 27001 to help all organizations that must comply with the regulation to comply with new European regulations for the protection of personal data.

This analysis is based on the experience gained in the implementation of ISO 27001 in organizations of different business areas and the establishment of compliance reports with GDPR.

The ISO 27001 standard is an excellent framework for compliance with EU GDPR. If the organization has already implemented the standard, it is at least halfway toward ensuring the protection of personal data and minimizing the risk of a leak, from which the financial impact and visibility could be devastating for the organization.

Introduction

The European Union General Data Protection Regulation (EU GDPR) will replace the actual Directive (Data Protection Directive 95/46/EC). It will not apply until May 25, 2018, but will require companies to prepare as soon as possible, taking into account some obligations may be expensive and the implementation will be time-consuming.

The new regulation introduces a set of rules, which require organizations to implement controls to protect personal data. Implementation of ISO 27001 will help organizations respond to this requirement.

What is personal data?

Based on the definitions in Article 2 of Directive 95/46/EC, personal data is any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.

Examples of personal data are ID card copy, image recorded in video surveillance cameras, and recorded voice. A list of customer names and addresses would count as personal data, as might a database of customer email addresses. It would not be considered personal data if it was not possible to determine in any way to which person the data refers.

What is EU General Data Protection Regulation (EU GDPR)?

Since 1995, European legislation has not updated the old directive (Data Protection Directive 95/46/EC) – that directive was converted into member countries, resulting in a differentiation of rules between the different countries of the European community.

This new regulation (EU GDPR) was approved on April 14, 2016, by the European Parliament and the Council of Europe. It will be applied directly in each country, exactly as it is, with the effect being that all the EU countries will have the same rights of citizens' privacy.

Some of the most relevant points of EU GDPR are the following:

- Taking into account the nature and purpose of data usage, both those who determine the purpose and means of the processing of personal data (Data Controllers), and who in turn manage the data (Data Processors), to be compliant with EU GDPR, will have to implement organizational measures and techniques to achieve an appropriate level of data security in terms of confidentiality, integrity, availability, and resilience of the systems that support them, as well as the regular validation of the effectiveness of these measures.
- Beyond the EU companies, the EU GDPR covers companies outside of the EU that monitor behavior or offer goods or services to EU Data Subjects ("an identified or identifiable person to whom the 'personal data' relate"), even if they offer this service for free.
- By the new regulation, organizations have to minimize data collection and retention and gain consent from consumers when processing data; in other words, they must minimize collection of consumer data, minimize with whom they share the data, and minimize how long they keep it. The goal is for organizations only to collect or store information they need for the purpose intended, particularly with regard to personal data.
- The EU GDPR has strengthened the previous directive, allowing the right to be forgotten by the personal data owners and requesting the deletion of their data by organizations, including published data on the web. EU GDPR states that "the (…) controller shall have the obligation to erase personal data without undue delay, especially in relation to personal data which were collected when the data subject was a child, and the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay."
- In case of a personal data breach, the company will have to notify the organization responsible for this purpose, the Data Protection Authority (DPA) ("national supervisory authority, acting with complete independence, responsible for monitoring the application of data protection rules at a national level"), within 72 hours after having detected the violation. Mandatory notification of affected individuals depends on the possibility of unauthorized access to information. Notification does not need to be made to the DPA if the breach is unlikely to result in a risk to the rights and freedoms of individuals.

- If the organization is dealing with special categories of personal data on a large scale, it needs to appoint a Data Protection Officer (DPO) as part of its board.
- If these measures are not met, the penalties are high – up to 20 million Euros or, in the case of companies, up to 4% of annual turnover, whichever is higher.

Controller vs. processor

There are two types of responsibilities regarding the protection of personal data: data "controllers" and data "processors."

Specifically, any business that determines the purposes and means of processing personal data is considered a "controller." Any business that processes personal data on behalf of the controller is considered a "processor." For example, a bank (controller) collects the data of its clients when they open an account, but it is another organization (processor) that stores, digitizes, and catalogs all the information produced in paper by the bank.

In fact, some organizations have no control over the data they store from their customers. The question is: within the EU GDPR, what are the responsibilities of these organizations if they store personal data? Are they covered by the new European regulations?

According to Article 4 of EU GDPR, different roles are identified as indicated below:

- Controller – "*means the 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*"
- Processor – "*means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*"

Both organizations are responsible for handling the personal data of these customers.

Does my organization need to be EU GDPR compliant?

First of all, it should be noted that the personal data of employees is included in the scope of this regulation.

The organizations that need to be EU GDPR compliant are:

- Companies (controllers and processors) established in the EU, regardless of whether or not the processing takes place within the EU.
- Companies (controllers and processors) not established in the EU offering goods or services within the EU or to EU individuals.

So, companies from anywhere in the world who employ European citizens or who process European citizens' data, collected through forms from their websites, need to be compliant. European companies processing personal data hosted outside Europe by European citizens need to be compliant. Even European companies employing non-European citizens need to be compliant. A non-European company that does not employ European citizens and does not store personal data of European customers will not be covered by the regulation.

What are the controllers' responsibilities?

According to Article 5 from EU GDPR, the controller shall be responsible for, and be able to demonstrate compliance with, the principles relating to processing of personal data: lawfulness, fairness and transparency, data minimization, accuracy, storage limitation and integrity, and confidentiality of personal data.

According to Article 24 from EU GDPR, "*Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*"

Examples of such measures may be the allocation of responsibilities for data protection, a data protection impact assessment and a risk mitigation plan, or the implementation of pseudonymization and data minimization in order to meet the requirements of this regulation and protect the rights of data subjects.

If there are several organizations that share the responsibility for the processing of personal data, EU GDPR includes the existence of joint controllers. They must determine their respective responsibilities by agreement and provide the content of this agreement to the data subjects, defining means of communication with processors with a single point of contact.

What are the processors' responsibilities?

According to Article 28 from EU GDPR, "*Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*"

This means that if any EU or non-EU company wants to stay in business, controllers or processors will have to implement the necessary controls to ensure that they comply with EU GDPR, because the fines can be applied to both controllers and processors. According to Article 83, fines shall be imposed regarding "the degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them."

How can organizations prepare?

The impact of EU GDPR means that personal data protection has to become a matter of vital importance for the top management of organizations. It is fundamental that policies be prepared based on an accountability framework and transparent rules to ensure rapid response to security incidents and consequent personal data leaks.

The adoption of standards such as ISO/IEC 27001 Information Security and, potentially, ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, will be the basis to quickly achieve compliance with the EU GDPR.

How are EU GDPR, ISO 27001 and 27018 related?

The ISO 27001 standard is a framework for information protection. According to EU GDPR, personal data is critical information that all organizations need to protect. Of course, there are some EU GDPR requirements that are not directly covered in ISO 27001, such as supporting the rights of personal data subjects: the right to be informed, the right to have their data deleted, and data portability. However, if an organization stores/processes personal data in the cloud, it can also use ISO 27018 to cover many EU GDPR requirements (See the article ISO 27001 vs. ISO 27018 – Standard for protecting privacy in the cloud to learn more). Therefore, if the implementation of ISO 27001 identifies personal data as an information security asset, and those that stores/processes personal data in the cloud follow ISO 27018 recommendations, most of the EU GDPR requirements will be covered.

The ISO 27000 series of standards provide the means to ensure this protection. There are many points where the ISO 27001 and ISO 27018 standards can help achieve compliance with this regulation. Here are just a few of the most relevant ones:

- **Risk assessment** – Because of the high fines defined in EU GDPR and major financial impact on organizations, it will be natural that the risk found during risk assessment regarding personal data is too high not to be dealt with. On the other side, one of the new requirements of the EU GDPR is the implementation of Data Protection Impact Assessments, where companies will have to first analyze the risks to their privacy, the same as is required by ISO 27001. Of course, while implementing ISO 27001, personal data must be classified as high criticality, but according to the control A.8.2.1 (Classification of information), "Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification." (Read the article ISO 27001 risk assessment & treatment – 6 basic steps to learn more.)
- **Compliance** – By implementing ISO 27001, because of control A.18.1.1 (Identification of applicable legislation and contractual requirements), it is mandatory to have a list of relevant legislative, statutory, regulatory, and contractual requirements. If the organization needs to be compliant with EU GDPR (see section above), this regulation will have to be part of this list. In any case, even if the organization is not covered by the EU GDPR, control A.18.1.4 (Privacy and protection of personally identifiable information) of ISO 27001 guides organizations in the implementation of a data policy and protection of personally identifiable Information. For cloud services providers, ISO 27018 control A.11.1 (Geographical location of PII) recommends that contractual agreements for international transfer of data must be available to cloud service customers.

- **Breach notification** – Companies will have to notify data authorities within 72 hours after a breach of personal data has been discovered. The implementation of ISO 27001 control A.16.1 (Management of information security incidents and improvements) will ensure "a consistent and effective approach to the management of information security incidents, including communication on security events." For cloud service providers, ISO 27018 has control A.9.1 (Notification of a data breach involving PII), with specific recommendations for preparation and handling of data breach incidents. According to EU GDPR, data subjects ("*a living individual to whom personal data relates*") will also have to be notified, but only if the data poses a "high risk to data subjects' rights and freedom." The implementation of incident management, which results in detection and reporting of personal data incidents, will bring an improvement to the organization wishing to conform to GDPR. (Read the article Enabling communication during disruptive incidents according to ISO 22301 to learn more.)
- **Asset management** – The ISO 27001 control A.8 (Asset management) leads to inclusion of personal data as information security assets, and allows organizations to understand what personal data is involved and where to store it, how long, its origin, and who has access, which are all requirements of EU GDPR. (Read the article How to handle Asset register (Asset inventory) according to ISO 27001 to learn more.)
- **Privacy by Design** – The adoption of Privacy by Design, an EU GDPR requirement, becomes mandatory in the development of products and systems. ISO 27001 control A.14 (System acquisitions, development and maintenance) ensures that "*information security is an integral part of information systems across the entire lifecycle*." For cloud service providers, ISO 27018 control A.4.2 recommends that secure erasure of temporary files should be considered as a requirement for information systems development. (Read the article How to integrate ISO 27001 A.14 controls into the system/software development life cycle (SDLC) to learn more.)
- **Supplier Relationships** – The ISO 27001 control A.15.1 (Information security in supplier relationships) aims for the "protection of the organization's assets that are accessible by suppliers." For cloud service providers, ISO 27018 recommends explicit definition of responsibilities of cloud service provider, sub-contractors, and cloud service customers. According to GDPR, the organization delegates suppliers' processing and storage of personal data, and it shall require compliance with the requirements of the regulation through formal agreements. (Read the article 6-step process for handling supplier security according to ISO 27001 to learn more.)

Is ISO 27001 enough?

In addition to the adopted technical controls, structured documentation, monitoring, and continuous improvement, the implementation of ISO 27001 promotes a culture and awareness of security incidents in organizations. The employees of these organizations are more aware and have more knowledge to be able to detect and report security incidents. Information security is not only about technology. It's also about people and processes.

The first thing an organization should do is an EU GDPR GAP Analysis to determine what remains to be done to meet the EU GDPR requirements, and then these requirements can be easily added through the Information Security Management System that is already set by ISO 27001.

From the ISO 27000 family, ISO/IEC 27018 should also be consulted (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors) if the organization stores/processes personal data in the cloud. See the article ISO 27001 vs. ISO 27018 – Standard for protecting privacy in the cloud to learn more.

To summarize, almost any company that is operating internationally will have to comply with this regulation. As ISO 27001 is internationally recognized and implemented all over the world, it may be the best option to facilitate immediate compliance with EU GDPR.

Conclusion

The implementation of ISO 27001 covers most of the requirements of the EU GDPR; however, some controls should be adapted to include personal data within its Information Security Management System.

In addition to what is planned for the implementation of ISO 27001, some measures will have to be included in order for an organization, either controller or processor, to ensure compliance with EU GDPR, such as Procedures for ensuring the exercise of the rights of data subjects, Mechanisms for the transfer of data outside the EU, Minimum content of the impact assessment on data protection, and Procedures to be followed in case of violation of personal data. All these controls can be integrated into the Information Security Management System, allowing the guarantee of legal compliance and continuous improvement, even more so when the ISMS and EU GDPR are aligned.

The organizations covered by the EU GDPR have until May 2018 to implement a set of measures that may imply a drastic change in their way of operating. Not knowing where to start can make this whole process unnecessarily complex. Therefore, the implementation of an ISMS compliant with ISO 27001 is a sure step for an organization to achieve compliance with EU GDPR.

Useful resources

- EU GDPR & ISO 27001 Integrated Documentation Toolkit – full set of documents with expert support.
- EU GDPR tool - access the full EU GDPR text arranged in chapters, articles, and sections making it easy to review and follow.
- ISO 27001:2013 Foundations Course – free online training that explains the basics of the standard, and the implementation steps.
- Conformio – online software that can be used as document management system (DMS) and provides a detailed list of ISO 27001 implementation steps.

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

Advisera Expert Solutions Ltd
for electronic business and business consulting
Zavizanska 12, 10000 Zagreb
Croatia, European Union

Email: support@advisera.com
U.S. (international): +1 (646) 759 9933
United Kingdom (international): +44 1502 449001
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Australia: +61 3 4000 0020

EXPLORE **ADVISERA**

9001 Academy · 9100 Academy · 13485 Academy · 14001 Academy · 16949 Academy · 18001 Academy

20000 Academy · 27001 Academy · Conformio · eTraining · AdviseraBooks

Advisera
Making certification simple.