Mapping of ISO 27001 to GDPR

Infopercept

Overview

What is GDPR?

Stronger rules on data protection mean people have more control over their personal data & businesses benefit from a level playing field.
The European Union's (EU) new General Data Protection Regulation (GDPR), regulates the processing by an individual, a company or an organization of personal data relating to individuals in the EU.

What is ISO 27001:2013?

ISO 27001 is an information security standard that helps companies come into compliance with international best–practice models. The standard covers three key components of data security: people, process, technology.

Infopercept

Literature Review

Company's critical data

ISO 27001 has a broader scope than GDPR in that it applies to a company's critical data as well as to personal data. GDPR also covers several areas that ISO 27001 doesn't.

ISMS can support

Though ISO 27001 doesn't explicitly address these rights, but an ISMS can support you in meeting these requirements.

GDPR-compliant.

Being certified to ISO 27001 doesn't necessarily ensure that you're also GDPR-compliant. It will certainly support you in your GDPR compliance goals and bring you closer to reaching them.

Infopercept

Purpose of the study

The purpose of the study is to identify whether being certified to ISO 27001:2013 is enough to be GDPR compliant or not.

Definitions

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.

A living individual to whom personal data relates is a Data Subject.

Organizations in scope of GDPR

The organizations that need to be EU GDPR compliant are companies' controllers and processors) whether established in the EU or not, offering goods or services within the EU or to EU individuals.

Organizations in scope of GDPR

Personal data that has been de-identified, encrypted or pseudonymized but can be used to re-identify a person remains personal data and falls within the scope of the GDPR. Anonymized data, i.e. data that cannot be reversed to identify an individual is not in scope.

DPAs (Data Protection Authorities)

GPDR requires many organizations to appoint DPAs with expert knowledge of the regulation and sufficient authority within the organization to advocate for data subject rights & to handle complaints lodged against violations of the GDPR & the relevant national laws.

Findings

How are EU GDPR and ISO 27001 related?

ISO 27001 is a framework for information protection. According to GDPR, personal data is critical information that all organizations need to protect.

Although they come from different perspectives, ISO 27001 and the GDPR at their core are both about reducing risk to people and organizations caused by misuse of personal data, with demonstrable overlap in both principles and requirements.

On the one hand, ISO 27001 focuses on reducing risks to information security by compelling organizations to produce information security management systems that are continuously maintained and improved.

On the other hand, the GPDR focuses on reducing risks for data subjects by providing them with rights, placing clear privacy responsibilities on organizations processing personal data, and holding them accountable through legal and administrative enforcement mechanisms.

Infopercept

How can ISO 27001:2013 help?

It's designed to support the confidentiality, integrity and availability of your information and help you maintain legal compliance. It helps you to protect your data from cyber-crimes, misuse, fire, theft and other threats.

Is ISO 27001:2013 Enough?

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.
So one needs to cover these rights in the policies for being

Infopercept

Mapping GDPR to ISO 27001

Following are six critical areas of common ground between ISO 27001 & GDPR :

1. Security

Conformity with ISO 27001 provides strong evidence of compliance with GDPR Article 32 security requirements. Both regimes focus on the risk associated with loss of CIA of protected data. Both regimes require internal leadership to work with other professionals throughout the organization to map data processing activities and assess risk to the organization & data subjects. Security professionals will work closely with the privacy team to provide documentation that security systems are appropriate to the risk.

2. Breach notification

- The implementation of ISO 27001 control A.16.1 (Management of information security incidents and improvements) ensures “a consistent and effective approach to the management of information security incidents, including communication on security events.”

- As per Article 33 of GDPR, any organization that collects the private data of users is required to report news of a data breach to a protection authority within 72 hours of
- when the breach first becomes known to the organization. Failure to do so could result in a fine of as much as 2% of a company's global annual revenue, or a fine of £10 million — whichever happens to be the larger amount.

- Article 34 of GDPR requires notification to data subjects following a breach when it results in a high risk to the rights and freedoms of natural persons. Notification must include the DPO’s contact information, the likely consequences of the breach, and the measures taken or considered to address the breach.

3. Vendor management /Supplier Relationships

ISO 27001 control A.15.1 (Information security in supplier relationships) requires the “protection of the organization’s assets that are accessible by suppliers.” According to GDPR, the organization delegates suppliers’ processing and storage of personal data; it shall require compliance with the requirements of the regulation through formal agreements.

4. Recordkeeping/Asset Management

- 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, what is its origin, and who has access, which are all requirements of EU GDPR.

- According to GDPR, a controller shall maintain a record of processing activities under its responsibility as well as a processor shall maintain a record of all categories of processing activities carried out on behalf of a controller.

5. Privacy by design

Privacy teams will likely engage security teams with evaluating existing collection and processing practices to determine whether the collection limitation principle is being appropriately considered. Security is a key component of privacy by design and privacy by default in product and system design.

The adoption of Privacy by Design, another 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.”

6. Data Subject Rights

- Privacy teams will need to work closely with security professionals to understand the categories of data collected and stored, and respective retention policies.
- Subject rights include being able to obtain a copy of their own info, what it is being used for, to whom it may be disclosed etc. Under GDPR details of the data “controller” and “data protection officer” are to be given to the subject whose data is been collected.
- People have the right to get their personal info corrected, completed, clarified etc.

Infopercept

CONCLUSION

1

The frameworks and policies already developed and implemented by security teams in ISO 27001 may streamline and significantly simplify the development of new GDPR-compliant privacy procedures.

2

Organizations that currently have an ISO27000 ISMS (Information Security Management System) are therefore likely
to have many of the GDPR requirements in place already but may need to make some adjustments.

3

The first thing an organization should do is conduct 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.

4

Gap Analysis Service assesses the extent of your organization’s compliance with the GDPR, and helps identify and prioritize the areas that it should urgently address.

Infopercept

THANK YOU

For More Information Please Visit our Website

www.infopercept.com