HOW IS THE EU GDPR LEGISLATION 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. ISO 27001 provides the means to ensure this protection. **The implementation of ISO 27001 identifies personal data as an information security asset and as such most of the EU GDPR requirements will be covered.**

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 there are many points where the ISO 27001 standard helps achieve compliance with this regulation. Here are just a few of the most relevant ones:

- **RISK ASSESMENT**
  Because of the high fines defined within EU GDPR and the major financial impact on organisations, it is only 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 analyse 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."

  ISMP005 CLASSIFICATION PROCEDURE
  SHIFT F7 RISK & OBJECTIVE REGISTER

- **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 an organisation 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 through the implementation of a data policy and protection of personally identifiable Information.

  ISMP003 LEGAL & OTHER REQUIREMENT POLICY

- **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." According to EU GDPR, data subjects ("The Data Subject is 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 subject's rights and freedom." The implementation of incident management, which results in detection and reporting of personal data incidents, will bring an improvement to the organisation wishing to conform to GDPR.

ISMP001 INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE
DATA BREACH POLICY & DATA PROTECTION POLICY

- **ASSET MANAGEMENT**
  ISO 27001 control A.8 (Asset Management) leads to inclusion of personal data as information security assets and allows organisations 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.

ISMO001 CONTROL OF DOCUMENTS & RECORDS
ISMP004 ASSET MANAGEMENT POLICY & PROCEDURE
IS SECURITY POLICY

- **PRIVACY BY 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."

ISMP013 PATCHING MANAGEMENT POLICY
ISMOP01 ACCESS CONTROL POLICY
ISMOP06 INFORMATION TRANSFER POLICY
ISMOP08 MOBILE COMPUTING/TELEWORKING POLICY

- **SUPPLIER RELATIONSHIPS**
  ISO 27001 control A.15.1 (Information security in supplier relationships) requires the "protection of the organisation'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.

  Suppliers of Shift F7 do not have access to the company's assets.

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

As ISO 27001 is internationally recognised and implemented all over the world, it is one of the best options to facilitate compliance with EU GDPR.