9 WAYS ISO 27001 HELPS YOU COMPLY WITH THE GDPR

ISO 27001 is an information security management standard that provides detailed guidance for taking the appropriate security measures, in the form of an information security management system (ISMS), to protect your business from a data breach.

An ISMS is a system of processes, documents, technology and people that helps to manage, monitor, audit and improve your organisation's information security practices. It helps you manage all your security processes in one place, consistently and cost-effectively.

Rather than implementing controls indiscriminately to reduce your data breach risks, by following a best-practice information security standard, you will be able to implement adequate and effective security measures, based on the outcomes of a formal risk assessment, to comply with the GDPR.

Here are nine ways ISO 27001 helps you achieve GDPR compliance.

1. ASSURANCE

The GDPR recommends the use of certification schemes such as ISO 27001 as a way of providing the necessary assurance that the organisation is effectively managing its information security risks.

2. NOT JUST PERSONAL DATA

ISO 27001 follows international best practice and will help you put processes in place that protect not only customer information but also all your information assets, including information that is stored electronically and in hard copy format.

3. CONTROLS AND SECURITY FRAMEWORK

The GDPR stipulates that organisations should select appropriate technical and organisational controls to mitigate the identified risks. The majority of the GDPR's data protection arrangements and controls are also recommended by ISO 27001.

4. PEOPLE, PROCESSES AND TECHNOLOGY

ISO 27001 encompasses the three essential aspects of information security: people, processes and technology, which means you can protect your business not only from technology-based risks but also other, more common threats, such as poorly informed staff or ineffective procedures.

5. ACCOUNTABILITY

ISO 27001 requires your security regime to be supported by top leadership and incorporated into the organisation's culture and strategy. It also requires the appointment of a senior individual who takes accountability for the ISMS. The GDPR mandates clear accountability for data protection throughout the organisation.

6. RISK ASSESSMENTS

ISO 27001 compliance means conducting regular risk assessments to identify threats and vulnerabilities that can affect your information assets, and to take steps to protect that data. The GDPR specifically requires a risk assessment to ensure an organisation has identified risks that can impact personal data.

7. CONTINUAL IMPROVEMENT

ISO 27001 requires that your ISMS is constantly monitored, updated and reviewed, meaning that it evolves as your business evolves using a process of continual improvement. This means your ISMS will adapt to changes – both internal and external – as you continually identify and reduce risks.

8. TESTING AND AUDITS

Being GDPR-compliant means an organisation needs to carry out regular testing and audits to prove that its security regime is working effectively. An ISO 27001-compliant ISMS needs to be regularly assessed according to the internal audit guidelines provided by the Standard.

9. CERTIFICATION

The GDPR requires organisations to take the necessary steps to ensure the security controls work as designed. Achieving accredited certification to ISO 27001 delivers an independent, expert assessment of whether you have implemented adequate measures to protect your data.

Implementing an ISMS conformant with ISO 27001 is not only information security best practice but also integral to demonstrate data protection compliance. Read more about ISO 27001.

Find out how to get started with ISO 27001 by speaking to one of our ISO 27001 experts today.