GDPR – GENERAL DATA PROTECTION REGULATION

WHAT YOU NEED TO KNOW ABOUT GDPR

As of 25th May 2018 GDPR will be enforced requiring UK organisations including SME's that process the personal data of EU residents to be compliant.
GDPR is a stronger requirement than the current Data Protection Act (DPA) which extends to the data rights of individuals and requires organisations to develop clear policies and procedures to protect personal data, adopting appropriate technical organisational measures.

Key changes include:

- ✓ If your business is outside the EU, you will still have to comply with the regulations if doing business with EU subjects personal data.
- ✓ The definition of personal data has become wider. Various factors will be used to identify an individual, such as their genetic, mental, economic, cultural or social identity.
- ✓ Parental consent will be required for the processing personal data of children under 16 years of age. EU member states may lower the age requiring parental consent to 13.
- ✓ The consent document must be laid out in clear and concise simple terms. Silence or inactivity does not constitute as consent. Clear processing of the private data must be provided.
- ✓ For certain companies a mandatory Data Protection Officer (DPO) will be required whereby the controller will be involved with regular and systematic monitoring of data subjects on a larger scale. Companies that are not data processing as their core business are exempt from this obligation.
- ✓ Data controllers will be required to conduct privacy impact assessments where privacy breach risks are high to analyse and minimise their risks to their data subjects.
- ✓ Data controllers will be required to report any data breaches to their data protection authority if it is deemed a risk to the right and freedoms of the subject in question. This must be made within 72 hours of the controller becoming aware of it, unless there are exceptional circumstances which will have to be justified.
- ✓ Regular supply chain reviews and audits will be required to ensure they are "fit for purpose" under the new regulations.
- ✓ Data subjects have the "right to be forgotten" Clear regulation guidelines are provided about these circumstances under which this right can be exercised.
- ✓ Since the regulation is also applicable to processors, organisations should be aware of the risk of transferring data to countries that are not part of the EU. Non EU controllers may need to appoint EU representatives if they wish to do business in the EU.

next connex

GDPR – GENERAL DATA PROTECTION REGULATION

- ✓ Data processors will share responsibility for protecting personal data. Processors will have a legal obligation and responsibilities, whereby the processor will be held liable for any data breaches. Contractual arrangements will need to be updated, responsibilities between the controller and processor will be an imperative requirement in the future. Parties will need to document their data responsibilities even more clearly.
- ✓ Data portability will allow a user to request copies of personal data in a usable format which is electronically transmissible to another processing system.
- ✓ Privacy by design is a concept that must consider compliance with the principles of data protection. The essence of privacy by design is that privacy in a service or product is taken in to account not only at the point of delivery, but also from the inception of the product concept. There is also a requirement that controllers should only collect data that is necessary to fulfil specific purposes and then discarding it when it is no longer required, to protect data subjects rights.
- ✓ A one-stop-shop approach for businesses means that companies will only have to deal with a single supervisory authority and not one for each of the EU's 28 member states, making it simpler and cheaper for companies to do business with the EU.

Penalties under GDPR

The new regulation mandates considerably tougher penalties than the DPA it replaces. Organisations found in breach can expect fines of up to 4% of annual global turnover or €20 million whichever is greater. Fines of this scale could very well lead to businesses insolvency.

ISO 27001 can help comply with data protection law now

ISO 27001 will help organisations protect their data assets and meet their compliance objectives now. An ISO 27001-compliant ISMS is a risk-based approach to information security management that addresses the specific security threats an organisation faces, covering people, processes and technology.

Accredited certification to ISO 27001 is recognised the world over as the hallmark of best-practice information security management, and demonstrates to customers, stakeholders and staff that an organisation takes its data security responsibilities seriously. The requirements for privacy seals – many of which will likely be covered by the Standard – can then be incorporated into the wider management system as they become available.

GDPR – GENERAL DATA PROTECTION REGULATION

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.

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.

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.

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.

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.

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.

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.

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.