European General Data Protection Regulation (EU GDPR)

How ISO/IEC 27001 certification with BSI can help

1,378,509,261 records breached in 2016

58.6% of incidents related to identify theft in 2016

3,776,738 records lost or stolen on average every day

1,792 Data breach incidents in 2016

Source: The Breach Level Index

We recognize that complying to privacy legislation, such as the new European General Data Protection Regulation (EU GDPR), is high on your business agenda. What can your organization do to prepare? Consider ISO/IEC 27001 certification with BSI.

An internationally recognized standard, ISO/IEC 27001 provides you with a best practice framework to manage your information security risks, including those related to personal information and privacy. It requires you to demonstrate that legal obligations, such as EU GDPR, have been considered and appropriately addressed. It also promotes secure design and accountability, which shows commitment to protecting information, including personal data.

What is EU GDPR?

The European General Data Protection Regulation (EU GDPR) is a new regulation around privacy of personal information that will be enforced from May 25, 2018. It aims to harmonize data protection law across the Single European Market, improve international business and reassure individuals that their information is protected.

Who does it affect?

- Both controllers and processors of personal data
- All EU member states, as well as any organization that operates within the EU market and has information on European data subjects

How does ISO/IEC 27001 support with EU GDPR?

Risk assessment

The high fines that will be enforced by the new regulations (up to €20 million or up to 4% of annual worldwide turnover of the parent company) could have a major financial impact on your organization. ISO/IEC 27001 requires you to conduct a risk assessment on your information assets, which should consider the increased risk to personal information and potential financial implications.

Compliance

The new law will be enforced from May 25, 2018 so you must review your obligations. ISO/IEC 27001 mandates that you have a list of and comply with relevant legislative, statutory, regulatory and contractual requirements.

Data classification

Personal data must be processed in a manner that ensures appropriate security. ISO/IEC 27001 requires organizations to ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

bsi.

...making excellence a habit.™

Reporting breach notification

Companies will have to notify data authorities within 72 hours after a breach of personal data has been discovered. ISO/IEC 27001 requires an incident management process to be put into place with information security events reported through appropriate management channels as quickly as possible.

Cooperation with authorities

Under EU GDPR, organizations must cooperate with the authorities e.g. privacy or data protection regulators.
ISO/IEC 27001 requires that "Appropriate contacts with relevant authorities shall be maintained".

Asset management

EU GDPR requires you to understand what personal data you collect, how it was obtained, where it's stored, how long it's kept for and who has access. ISO/IEC 27001 needs you to identify organizational assets and define appropriate protection responsibilities. You must complete an inventory of assets, understand who owns the assets, what is the acceptable use of those assets and how you are going retire the assets.

Privacy by design

The adoption of privacy by design is another EU GDPR requirement. ISO/IEC 27001 ensures that information security is designed and implemented as an integral part of the entire development and lifecycle of information systems.

Supplier relationships

EU GDPR applies to suppliers who process personal data on behalf of others; it requires controls and restrictions to be included in formal agreements. This applies to ISPs, CSPs and outsourced data centers ISO/IEC 27001 requires the protection of the organization's assets that are accessible by suppliers and for organizations to monitor the service delivery of suppliers against information security requirements.

Documentation

Under EU GDPR, controllers must maintain documentation concerning privacy e.g. for the purposes for which personal information is gathered and processed, "catagories"of data subjects and personal data. ISO/IEC 27001 requires documentation to be kept based on the complexity of processes and their interactions.

Is there anything else I need to consider above and beyond ISO/IEC 27001?

ISO/IEC 27001 is a great framework to demonstrate that you are committed to information security and privacy. It supports many of the EU GDPR requirements, however, you should also consider:

- **Training and awareness**
  Make sure your business leaders and key stakeholders are aware of this change in law. You need to help them understand the potential impact and may be required to provide more in-depth training.

  If you want to be more knowledgeable, we have a range of data protection courses you may want to consider, such as our EU General Data Protection Regulation foundation training.

- **Designate a Data Protection Officer (DPO)**
  Certain activities, such as large scale monitoring of individuals or processing of special category data, require an organization to appoint a DPO. Even if you don't need to, it's good practice to appoint a DPO with knowledge of information security and an understanding of data protection law.

- **Look at your procedures**
  Make sure you have procedures that cover all the rights individuals have. This includes how you ensure personal information is accurate, used for the purpose for which it was collected and not retained for longer than is necessary, as well as how you'd provide or delete personal data if requested to do so.

- **Enhance your system**
  If you're processing or storing information in the public cloud, ISO/IEC 27018 can also help. It builds upon an ISO/IEC 27001 system and ensures you put specific requirements in place to protect personally identifiable information.

Want even more guidance?
BS 10012 is the best practice framework for a personal information management system. It has recently been updated to more closely align with the EU GDPR requirements. You may wish to consider this as a supporting document or as an additional management system to put in place.

Why BSI?

We have been at the forefront of information security standards since 1995, having produced the world's first standard BS 7799, now ISO/IEC 27001. And we haven't stopped addressing new and emerging issues such as cyber and cloud security. That's why we're best placed to help you manage privacy and respond to regulations.

bsi.

To find out more
Call: **1 800 862 4977**
Visit: **bsigroup.com/en-US**