European General Data Protection Regulation (EU GDPR)

What does it mean for you as a BSI ISO/IEC 27001 certification client?

At BSI, we recognize that complying to the new European General Data Protection Regulation (EU GDPR) is high on your business agenda. In order for you to maintain a compliant ISO/IEC 27001 Information Security Management System (ISMS), you must demonstrate that you've considered and appropriately responded to this new legal requirement. But what exactly does this mean to your organization that already has a robust information security system in place?

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 and put individuals back in control of their personal data. It will help 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

What do I need to focus on?

You should already have many of the requirements in place; however, here are some of the areas we would encourage you to review to support meeting the EU GDPR requirements.

Risk assessment

The high fines that may be imposed 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. This places a greater risk on the personal information your organization stores.

Compliance

The new law will be enforced from May 25, 2018 so you must review your obligations. ISO/IEC 27001 control A.18.1.1 (Identification of applicable legislation and contractual requirements) mandates that you have a list of relevant legislative, statutory, regulatory and contractual requirements.

Data classification

Personal data must be processed in a manner that ensures appropriate security. ISO/IEC 27001 control A.8.2 (Information classification) requires organizations to ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

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 control A.16 (Information security incident management) requires an incident management process to be put into place with information security events reported through appropriate management channels as quickly as possible.

bsi.

...making excellence a habit.™

Cooperation with authorities

Under EU GDPR, organizations must cooperate with the authorities e.g. privacy or data protection regulators. ISO/IEC 27001 clause 6.1.3 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 control A.8 (Asset management) is about "information assets," which includes personal data. The objective is 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 to retire the assets.

Privacy by design

The adoption of privacy by design is another EU GDPR requirement. ISO/IEC 27001 control A.14 (System acquisitions, development and maintenance) 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 control A.15.1 (Information security in supplier relationships) requires the protection of the organization's assets that are accessible by suppliers, and A.15.2 (Supplier service delivery management) states that organizations need to monitor the service delivery of suppliers against information security requirements.

Documentation

Under EU GDPR, controllers must maintain documentation concerning privacy e.g. the purposes for which personal information is gathered and processed, 'categories' of data subjects and personal data. ISO/IEC 27001 control 7.5 (Documented information) 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?

While ISO/IEC 27001 supports you with many of the EU GDPR requirements, 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 feel more knowledgeable, we do 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.

- **Internal audit** – Use your internal audit to assess what personal data you hold, where it came from and with whom you share it.

- **Review procedures** – Ensure your procedures 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.

- **Review your incident management process** – Make sure that you can respond in the tight timescales required by the new regulation should a personal information incident occur.

- **Review your system** – Depending on the scope of your ISMS and the controls you've implemented, there may be additional guidance that can help such as BS 10012 and ISO/IEC 27018.

  BS 10012 outlines the requirements for a personal information management system. It's recently been updated to align with the EU GDPR requirements. You may wish to consider this as a supporting document or an additional management system to put in place.

  Also if you're processing or storing information in the public cloud, ISO/IEC 27018 can help. It builds upon your existing ISO/IEC 27001 system to put specific controls in place to protect personally identifiable information.

bsi.

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