Grant Thornton
An instinct for growth™

Information Security

BS 10012

The official British Standard for data protection

March 2018

3576GT-03-18

What is BS 10012?

BS 10012:2017 is the latest release of a British Standard entitled *Data protection – Specification for a personal information management system*. Published in March 2017, this new version of the standard incorporates two key changes from the previous (2009) edition:

- The content has been revised so it aligns perfectly with the requirements of the General Data Protection Regulation (GDPR).
- The structure has been updated to match that of ISO standards such as the ISO 27000 series of information security standards.

Why would I adopt BS 10012?

In order to comply with the requirements of GDPR, it is essential that your organisation has strong, effective controls around how personal data is stored, managed and processed: a solid data protection regime that is implemented and understood throughout the organisation provides excellent protection against the risk of a data breach.

ISO 27001 is a solid choice for implementing controls, but for many organisations it is overkill: it provides a framework for an information security management system that spans all aspects of security. BS 10012, on the other hand, is targeted specifically at the management of personal data – the core focus of the GDPR legislation – and as such it is a much more appropriate standard if your focus is specifically on the protection of personal data.

Is it a global standard?

The "BS" prefix denotes that it's presently a British Standard. We are convinced, however, that it will be adopted very soon as a global ISO standard. This is precisely what happened in the case of ISO 27001, in fact: it began in 1995 as BS 7799 and ten years later was transformed into ISO 27001.

How does BS 10012 differ from GDPR?

GDPR is a piece of legislation: it defines what behaviour is and is not permitted when handling personal data, and provides for financial and other sanctions that can be imposed on organisations that behave improperly.

BS 10012, on the other hand, is a framework that you can use to build a Personal Information Management System (PIMS) in order to comply with the law and be able to demonstrate that compliance. It details all the ingredients of a system of personal data controls – from producing registers of interested parties and defining the roles and responsibilities of individuals through to writing policies and procedures, providing training and awareness, and monitoring your compliance with the law.

Also worthy of note is that BS 10012 is an independently auditable standard. That is, you can engage a certified external auditor to evaluate your compliance and, if satisfied, issue a certificate to confirm this. There is currently no such thing as a "GDPR compliance certificate" for an organisation – and it is likely that the ISO standard into which BS 10012 evolves will become the *de facto* compliance certificate for data protection.

Accreditation or compliance

As with ISO 27001, organisations may choose to adopt working practices that align with the requirements of BS 10012 without obtaining formal accreditation. Even without independent scrutiny, the organisation will inevitably benefit from working according to a robust, comprehensive standard.

What Grant Thornton can do for you

Our compliance specialists will:

- Work with you to investigate the best standard for your controls on personal data.
- Carry out risk assessments.
- Define the scope and plan the implementation of your PIMS.
- Produce and implement the controls that will form your PIMS.
- Educate your staff to ensure they are able to work efficiently within the PIMS.
- Provide gap analyses and pre-audit evaluations to measure your level of conformity prior to formal audit.
- Arrange and oversee the formal external audit process.
- Define and implement a regime of continual improvement.

For more information please contact:

David Cartwright
Senior Consultant, Information Security
T +44 (0) 1534 885813
E david.cartwright@gt-ci.com

Grant Thornton

An instinct for growth™

grantthorntonci.com