ISO 27001 readiness for GDPR and the DPA 2018

A quick surf of the internet lists many articles demonstrating how ISO 27001 can help you to be ready for General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA), usually from companies only too glad to help you implement ISO 27001. In this article, I would like to take a slightly different tack, and look at some of the things you must consider when updating your Information Security Management System (ISMS) to encompass the requirements of GDPR.

General Data Protection Regulation (GDPR)

The GDPR is a piece of European legislation designed to give commonality of data protection laws across the EU. The Regulation came into force on 5th May 2016, and businesses were required to be compliant by May 2018. It was incorporated into United Kingdom law as the Data Protection Act 2018, thus answering any questions as to whether GDPR may not be applied post-Brexit.

The new legislation has introduced some significant changes, including breach notification requirements and data portability, but I do not intend to give a lengthy explanation of all the requirements of the Regulation in this article; the Information Commissioner's Office (ICO) has produced a useful guide, 'Preparing for the General Data Protection regulation (GDMR): 12 Steps to Take now', and there are other useful resources on the internet. However, I will discuss some of the requirements, and their relationship with ISO 27001, in more detail below.

GDPR & DPA Requirements

The principles of the GDPR require that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

An ISO 27001-compliant ISMS would normally comply with these principles, which could be summarised by Confidentiality, Integrity and Availability. However, it is the later, more detailed

clauses where changes may be required. Here, I consider some of the requirements of GDPR, and where your ISMS may need updating:

Accountability

Accountability is a significant element of the new DPA , which requires that you have governance measures in place. ISO 27001 will ensure that you have many of these requirements already present, but you will need to add in Data Protection Impact Assessments (DPIA), which will include at least 'an assessment of the risks to the rights and freedoms of data subjects'. You may additionally need to review whether your KPIs, or equivalent, comply with requirements such as documentation, staff training and awareness.

Breach Notification

The DPA requires that certain types of breaches must be reported to the relevant authority and, in some cases, to the individuals affected. This could require a change to your events and incident management processes (Control A.16.1), not least to ensure a swift and effective decision-making and reporting procedure. The ICO also points out that you need to ensure that 'your staff understands what constitutes a data breach, and that this is more than a loss of personal data'.

Risk Assessment

GDPR and the DPA require that organisation complete a 'Data Protection Impact Assessment' (DPIA). ISO 27001 does require that organisations determine 'the requirements of interested parties relevant to information security', but organisations may now need to consider whether their risks assessments effectively cover the requirements of a Privacy Assessment, or whether this is something that will additionally need to be completed.

Data Portability

Data portability enables people to request and re-use their personal data, with the data being provided free of charge in a commonly used format, such as a .csv file. To enable this, your ISMS will need to be adapted to ensure that you are able to manage requests, accurately collate and then transmit this information within specific timelines.

Data Protection Controllers and Processors

The definitions for data protection controllers and processors has changed little, although there will be specific legal obligations for processors, with significantly more legal liability. As a controller, there are increased obligations to ensure that your processors are complying. This will have implications in several areas of an ISMS, such as ensuring relevant competencies and awareness; confirming that controls are adequate and maintaining records of data and processing activities.

Summary

The very fact that an organisation has ISO 27001 will mean that you are better prepared for the requirements of GDPR and the DPA. However, there are several areas of your ISMS that will have to be reviewed in the light of the requirements of the GDPR.