ALAN CALDER

NOT JUST BOX TICKING

Alan Calder examines what boards and senior managers must do to meet their obligations under the GDPR

The EU General Data Protection Regulation (GDPR) will mark a wide-reaching and significant shift in the way organisations protect personal data when it comes into effect in May 2018. Not only does the regulation apply to all EU data controllers and processors, it also applies to organisations outside the EU that deal with EU residents' personal data. Moreover, the government has confirmed the UK will adopt the regulation irrespective of Brexit.

Under the GDPR, data subjects have a number of new rights, including the right to judicial remedy against organisations that have infringed their rights (Article 79). On top of this, controllers face the possibility of administrative fines of up to €20m (£16.9m) or 4% of global annual turnover. These are intended to be "effective, proportionate and dissuasive" (Recital 151) – sending a clear message to organisations throughout the EU that they must take data protection seriously.

Failing to report a data breach to the regulator within 72 hours of discovery (or, if you report it after 72 hours, failing to explain the delay) represents another breach of the GDPR. So you can assume that the size of the administrative fines levied on you will be that much higher when any unreported breach is subsequently discovered, as it most surely will be.

CULTURE OF PRIVACY

If we're honest, most organisations' approach to data protection is very much a box-ticking exercise. However, as information commissioner Elizabeth Denham explained to ICAEW members on 17 January (for more about the event, see page 12), rather than just box-ticking, companies should focus on a "framework that can be used to build a culture of privacy that pervades an entire organisation". The key question is how can this be achieved?

Article 5 of the GDPR states that "the controller shall be responsible for, and able to demonstrate compliance with" six privacy principles. The sixth principle (integrity and confidentiality) states that personal data shall be "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".

One way for data controllers to demonstrate they are processing data in such a manner is to achieve certification to a recognised standard or framework.

The UK government's Cyber Essentials scheme sets out five security controls that organisations can implement to protect themselves from up to 80% of common cyber attacks, and certification to the scheme demonstrates independent verification that systems and applications have a base level of cyber security.

THE PROFESSIONAL APPROACH

Cyber Essentials only provides a snapshot of corporate security, however. Organisations seeking a greater level of information security maturity might turn to an international standard such as ISO 27001. An ISO 27001-compliant information security management system (ISMS) is a risk-based approach to information security that all organisations can use to demonstrate GDPR compliance. It has the added advantage of being an international standard against which organisations can achieve independently audited certification to demonstrate that they have implemented, and maintain, a system that addresses the specific information security risks that they face.

An ISMS supports both the privacy by default and by design principles, covers the necessary policies and procedures, provides a framework for staff training and incident response. Most importantly, it also sets out a best-practice approach to protecting personal data.

Under the GDPR, organisations have to be able to demonstrate that they have put in place proper accountability processes to ensure that they deal with the rights of data subjects in an appropriate manner. There are, of course, other steps that organisations can and should take to ensure their compliance, including appointing a data protection officer. But ISO 27001 certification provides a structure on which other activities depend. ●

Alan Calder, CEO, IT Governance