How a new regulation will change data protection in the EU

Q: From higher fines to new notification requirements, what should risk managers know about the forthcoming changes to data protection legislation?

A: Current data protection legislation in EU member states is derived from Directive 95/46/EC, which came into force in 1995.

However, since this time, there have been major technological developments and changes in the way in which data is used. By way of example, when the Directive was under development, the internet was still a relatively new phenomenon and social networking sites, location-based services or cloud computing did not exist. Twenty years on, a new law that specifically addresses the use of personal data in today's world and beyond is required.

Regulation v Directive

The proposed new legislation is in the form of a regulation, which differs from a directive.

A directive sets out a goal that all EU countries must achieve, but leaves it to the individual countries to decide how to do so. For this reason, current data protection legislation varies between member states as each has implemented the Directive into their national laws slightly differently. This has led to difficulties for international businesses that operate across a number of EU jurisdictions because they have to comply with slightly different requirements in each country.

In contrast, a regulation is binding and must be applied in its entirety across the EU. Here, this means that, once the Regulation has come into force, one set of rules should govern data protection in all member states.

Key changes

The Regulation will introduce numerous changes that cannot all be covered in this article. Some of the changes likely to have the greatest effect on businesses or that have been particularly high profile, are described below:

- **higher fines:** fines will be significantly increased. Current proposals range from between 1%-5% of an organisation's annual worldwide turnover or up to €1m, whichever is greater;
- **data protection officers:** certain organisations will have to appoint a data protection officer. The threshold for triggering this requirement is not yet confirmed; current proposals include having at least 250 employees or processing data of at least 5,000 individuals;
- **territorial scope:** the Regulation will in some circumstances apply to data controllers that are not based in the EU. This will be the case if a data controller:
  - processes personal data of individuals residing in the EU; and
  - such processing activities relate to offering them goods or services or monitoring their behaviour;
- **one supervisory authority:** there will be a "one-stop shop", that is one data protection authority will be responsible for the supervision of a business across all its EU operations. The supervisory authority that will be responsible for a business will be the one in the country of that business's main establishment. This will be the country in the EU where the main decisions about the processing of personal data are taken;
- **notification of data breaches:** the Regulation introduces an obligation to notify the supervisory authority of personal data breaches. A personal data breach is a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed";
- **consent:** where consent from individuals is used to justify the processing of their personal data, only express consent will be valid. Businesses will no longer be able to rely on implied consent; and
- **right to be forgotten:** individuals will have the right to require businesses to erase their personal data where the individual withdraws consent or objects to the processing on certain grounds. If the business has made the data public, it will have to make reasonable efforts to inform third parties of the request to delete any links to, or copies of, the data.

What next?

At present, the Regulation is still in draft form. Based on the current timetable, a final text is likely to be approved at some point this year. The Regulation will then come into force following a transitional period of two years to give businesses time to understand the new requirements and make any necessary changes.

In the meantime, businesses can prepare by making sure they have a good understanding of the ways in which personal data is used within their organisation, including how it is obtained, shared, transferred, retained, destroyed etc. Once data flows are mapped out, the business should ensure it has a robust internal governance framework with the necessary policies and procedures, and appropriate controls in place. Every business processing personal data should ensure that a designated person has responsibility for data protection across the business. Training should be rolled out along with initiatives to raise staff awareness of the relevant issues.

Robyn Palmer is a senior associate in the intellectual property and technology group at DLA Piper