New European Data Protection Laws

Published by 1 February 2016

In Compliance/Governance/Risk Management, Storage Technology,

Authored By: Pulina Whitaker and Lee Harding, Morgan Lewis.

Data protection and cyber security issues are becoming increasingly topical. There are news reports of cyber-attacks affecting customers almost daily. At the same time, European Union legislators have been looking to implement significant and far-reaching reforms in the areas of data protection and cyber security to ensure that legislation keeps pace with technological developments.

Existing data protection laws

Once viewed as the gold standard for data protection, Directive 95/46/EC (the "**Data Protection Directive**") is now seen by some as no longer fit for purpose in the wake of rapid technological development.

Currently, the Data Protection Directive provides a framework across the European Economic Area ("EEA"). As directives are implemented by the local law applicable in each European Union ("EU") country, there are variations in the way the Directive has been implemented. For global companies operating in multiple EU countries, this has increased the cost and complexity of doing business.

Proposed new General Data Protection Regulation

It is proposed that the new General Data Protection Regulation (the "Regulation") will be adopted by the end of 2015 or early 2016. The new Regulation will then take effect after a two year transitional period. Unlike directives, regulations are directly applicable. This means that they immediately take effect at the designated time without the need for local law in each EU country.

The Regulation will allow businesses operating across multiple EU countries to deal with just one data protection authority. The hope is that this will create a one stop regulatory shop. To reduce the risk of inconsistency, a European Data Protection Board will be created. The idea is that this Board will be able to give an opinion on cross-border data protection issues and approve measures to be adopted by data protection authorities.

Despite the potential for improvement of the current fragmented regulatory approach under the Data Protection Directive, consistency and certainty of approach may not strictly follow under the Regulation. The terminology of the Data Protection Directive has largely been retained under the Regulation. For example, in the absence of definitive court rulings from the Court of Justice, there is likely to be significant differences in the way that countries interpret 'personal data' and 'data subjects'.

Another potential issue is that there is little agreement between the three EU legislative bodies responsible for adopting the Regulation. This is likely to result in the European Commission, European Parliament and European Council agreeing to a form of wording that they can all live with rather than word which is necessarily appropriate. Unlike the Data Protection Directive, the Regulation will apply to all businesses based in the EU regardless of where the actual processing occurs, as well as any businesses which target EU consumers even if those businesses have no physical presence or employees in the EU. This development is likely to impact heavily on online businesses operating from outside the EU although there likely to be practical problems in enforcing these provisions.

The Regulation echoes the Data Protection Directive by requiring businesses to process personal data fairly and lawfully. Generally, this means processing with the consent of the individual or having a legitimate business justification to do so as well as undertaking the processing in a proportionate manner. For example, this might include obtaining the specific, informed and freely given data of an individual and notifying him/her of the purposes of the processing. Personal data should be accurate, kept up to date, retained securely and only for only so long as is necessary for the purposes of the processing. There is also a general prohibition on the cross-border transfer of personal data except for some limited exceptions.

The Regulation, in some other respects, goes beyond the existing levels of protection. The new requirements for businesses include:

- Ensuring that new IT systems are designed in a way that protects privacy from the outset (rather than being bolted on afterwards);
- Imposing default privacy-friendly settings on websites from the start of a user's experience;
- Rectifying and erasing personal data held about individuals on request (known as the right to be forgotten);

- Providing individuals with a copy of their personal data in are usable and electronic format on request;
- Appointing a data protection officer (this applies to large organisations or where data processing is a core function);
- Not taking measures in relation to individuals based solely on automated processing save for limited circumstances (this is significant for businesses based on big data solutions); and
- Reporting data security breaches to data protection authorities and affected individuals.

The Regulation will also increase accountability and introduces heavy fines of the greater of one million Euros or 2% of annual worldwide turnover for breaches.

Network and Information NIS Directive

Another major development is the Network and Information NIS Directive (the "**NIS Directive**"). This is in draft form and expected to become law by the end of2015 or early 2016. The NIS Directive will apply to certain businesses providing a "critical infrastructure service" in the EU including businesses in the energy, banking and health sectors. The NIS Directive proposes a number of measures with the aim of making the EU one of the safest cyber security environments in the world. This is a bold statement given that cyber-crime I one of the fastest growing forms of crime with over one million victims daily across the world.

Separately, the UK, like many EU countries, has its own cyber security strategy. The UK Government is committed to spending £650million on cyber security. A national cyber-crime unit was established in 2013and significant funds have been given to Oxford University as part of various research projects. The Financial Conduct Authority is also assessing the cybersecurity plans of major financial institutions.

In the event that a business experiences a beach of its data security system, it will be judged by the reasonableness of its efforts to prevent and mitigate incidents. Accordingly, a comprehensive, well-implemented incident response plan is critical for an organisation to demonstrate that it takes privacy and security seriously. Some businesses are also protecting themselves by taking out appropriate cyber insurance policies.

Data transfers to the US

After the European Court of Justice's ("ECJ") decision in Schrems, which declared that the EU-US Safe Harbor programme was invalid, the European Commission has committed to provide guidance to organisations on how to transfer personal data to the US by the end of July2016. There has been some recent discussions by the European Commission about anew "Safe Harbor 2.0" which, however, may not go far enough to deal with the concerns raised by the ECJ. In the meantime, organisations can consider model clauses or Binding Corporate Rules to transfer personal data to the US if they do not have consent from the individual to do so.

Reported by: Roger Buhlert – Cardinia Shire Council