ARNOLD & PORTER (UK) LLP

ADVISORY February 2012

Europe Announces Long-Awaited Plans to Reform the EU Data Protection Regime

On 25 January 2012, the European Commission announced plans to reform comprehensively the existing data protection regime across the 27 member states that form the EU. The proposals, in the form of a new Regulation, aim to modernise, reinforce, and future-proof the principles set out in the 1995 Directive (95/46/EC). However, with increased obligations, accountability, and serious bite in the form of fines for noncompliance, businesses should take heed and plan for the arrival of the new legislation as early as 2014.

Time for change

One of the criticisms commonly levelled at the existing EU data protection regulatory framework is that it is woefully outdated. Designed some 17 years ago in an age where less than one percent of Europeans used the Internet, legislators could not have predicted the vast growth and development of digital technology, electronic communications, and e-commerce, coupled with the fact that data has become a key commodity for business. The time is ripe for change.

A second criticism is that the existing framework is a patchwork of 27 national laws each implementing the 1995 Directive in a different way. The new proposals therefore take the form of a directly applicable Regulation, which will sweep away the national laws in favour of a single EU law, valid across all 27 EU member states. This will, it is hoped, end some of the legal uncertainty and costly administrative burdens that companies of all sizes face when doing business in Europe.

New developments

The new proposals are wide-ranging, although predominantly aimed at improving personal data protection for individuals and increasing accountability for those who process personal data (the "**data controllers**"):

- There will be a "**right to be forgotten**". This will enable individuals to withdraw their consent to the processing of their data at any time and request that all their personal data be deleted where there are no legitimate grounds for data controllers to retain it. This right could prove onerous and costly for businesses that process large volumes of personal data or rely on personal data as a core asset;
- Data controllers will need to obtain individuals' **explicit consent** before processing their data. This means that there will need to be some form of communication flowing from the individual that expressly permits the data controller to use their data (e.g., a

Contacts

Richard Dickinson
+44 (0)20 7786 6213

Henry Clinton-Davis
+44 (0)20 7786 6137

Nancy L. Perkins
+1 202.942.5065

Jake Marshall
+44 (0)20 7786 6219

Gemma Davies
+44 (0)20 7786 6195

tick box, pop-up window, or an email), instead of consent being assumed as is often the case at present;

- Individuals will have greater access to their own data and will be able to transfer personal data from one service provider to another more easily (known as the "**right to data portability**");
- The EU rules will be extended to cover personal data of individuals in the EU even where that data is **processed outside the EU**. This means that businesses that are not located in Europe (the business proper, or their servers) will still need to comply with EU rules where they offer goods or services to consumers in the EU or monitor EU consumers;
- Data controllers will be required to **notify any serious data security breaches** to their national data protection authority as well as the individuals concerned. This proposal is likely a reaction to the increase in large-scale security breaches in recent years, such as the hacks on the Sony Playstation network in 2011, which compromised the security of the company's 77 million users' data;
- Data controllers with more than 250 employees will be required to appoint a **data protection officer** to monitor and ensure compliance with data protection obligations; and
- A serious (intentional or negligent) failure to meet data protection obligations could attract **fines** of up to €1millon or two percent of an organisation's annual worldwide turnover.

Impact for business

The proposals will undoubtedly prove more onerous and expensive for business, as most areas of compliance are set to increase. Businesses will need to monitor actively their compliance, undertake impact assessments, maintain satisfactory audit trails, document their personal data processing activities and notify of data breaches.

However it is not all doom and gloom, and several proposals could prove beneficial for business such as:

- Improvements to the current system of binding corporate rules necessary for the global processing of EU-originated personal data to make it more straightforward and less onerous for worldwide businesses to obtain the necessary approvals to enable international data transfers;
- The development of the single EU law, which should in theory make it more straightforward to trade in Europe; and
- The removal of the requirement to notify the data protection authorities in each member state in which the company or organisation operates of its data processing activities. Instead, organisations will only have to deal with the data protection authority of the member state in which it has its main establishment.

The European Commission has estimated that the proposals will save businesses around €2.3billion per year. Whether this is a realistic projection is not yet known, but it may not be of much comfort to businesses in the face of increased regulatory burdens and hefty fines.

Implementation and timetable

The proposals will now be passed to the European Parliament and the EU member states for consultation, a process which can take over a year to complete. There will likely be some modification and refinement to the proposals during this period. Once agreed, the new Regulation will take effect two years from the date of adoption and will apply to all 27 EU member states automatically, without the need for any implementing legislation at a national level. Therefore the earliest that we can expect to see the proposals implemented is 2014, although a more realistic estimate is 2015.

We hope that you have found this Advisory useful. If you have additional questions, please contact your Arnold & Porter attorney or:

Richard Dickinson
+44 (0)20 7786 6213
Richard.Dickinson@aporter.com

Henry Clinton-Davis
+44 (0)20 7786 6137
Henry.Clinton-Davis@aporter.com

Nancy L. Perkins
+1 202.942.5065
Nancy.Perkins@aporter.com

Jake Marshall
+44 (0)20 7786 6219
Jake.Marshall@aporter.com

Gemma Davies
+44 (0)20 7786 6195
Gemma.Davies@aporter.com