Alerts and Updates

European Commission Issues New Data Protection Proposals

January 25, 2012

Much as was anticipated, the European Commission (the "Commission") announced its long-awaited proposals on what are likely to be viewed as drastic changes to data protection law in Europe. The proposals seek to make EU privacy laws fit for the 21st Century and seek to both change the system and increase penalties for breach, with fines of up to 2 percent of a corporation's annual global turnover. They also seek to introduce data breach laws similar to those which exist in most U.S. states, but possibly with a requirement to report a breach within 24 hours.

The European Union (EU) introduced the initial Data Privacy Directive (the "Directive") in 1995, although a number of European countries had their own data protection laws that pre-date the Directive. The Directive sought to give each country in the EU a template to follow for its own data protection laws. Theoretically, the law in each country must include the provisions mandated by the Directive, although additional measures are also permitted over and above the requirements of the Directive. Implementation and enforcement is left to each country in the EU, which has led in some instances to conflicts, complexity and inconsistencies.

The European Commission today proposed a comprehensive reform of the 1995 rules to try and bring in more uniformity. The regulation does not appear to be written in the most helpful language. The Commission's undated draft stretches to 119 pages. In addition to greater penalties and the new security breach laws, the new proposals have a number of interesting elements, including:

- A single set of rules on data protection across all of the EU.
- The requirements to register data collection and transfer in each country may be removed. Organizations will deal with a lead country that will regulate their activity across the EU. Investigations however are likely still to be conducted by the regulator where the complainant is based. How this might work in practice is not yet known. Companies based outside of the EU may wish to start thinking about these proposals in particular, given that some countries may still be more attractive than others, especially to U.S.-based corporations.
- A "right to be forgotten" will be introduced. This proposal has been discussed by leading figures at the Commission for some time and was originally aimed at social media, but it is likely to be of much wider effect. This may necessitate careful thought. For example, can an employee suspected of theft exercise his or her "right to be forgotten" to have those details deleted?

- The proposed new rules will have extra-territorial reach. EU laws will apply if personal data is handled abroad by companies that are active in the EU market and offer their services to EU citizens.

- The Commission wants national data protection authorities to be strengthened so they can better enforce the new rules. They will be empowered to fine companies that violate EU data protection rules. This can lead to penalties of up to €1 million or up to 2 percent of the global annual turnover of a company.

- Making data processors have direct responsibility for their actions.

- The introduction of a corporate data protection officer with specific responsibilities. This role exists (albeit on a voluntary basis) in Germany, but the proposal is to extend this to other EU countries.

- The abolition of the fee for subject access requests and increased penalties for failure to respond to a request. These penalties could be between 0.5 percent to 2 percent of global annual turnover. These changes, together with the introduction of the right to be forgotten, are likely to lead to significantly more requests from individuals for access to their data. Most companies will have to staff up to deal with these requests.

It is also proposed that some activities which are thought to be a particular concern for privacy are more heavily regulated. This list includes:

1. data mining and predictions based on that data

2. health and epidemiological data

3. CCTV and video data

4. genetic or biometric data

Initial reaction has been mixed. Even national regulatory authorities have concerns. For example, the UK Information Commissioner has said:

". . . in a number of areas the proposal is unnecessarily and unhelpfully over prescriptive. This poses challenges for its practical application and risks developing a 'tick box' approach to data protection compliance. The proposal also fails to properly recognise the reality of international transfers of personal data in today's globalised world and misses the opportunity to adjust the European regulatory approach accordingly."

Extraterritorial scope

The proposed new rules will have extraterritorial reach. EU rules must apply if personal data is handled abroad by companies that are active in the EU market and offer their services to EU citizens.

Article 3 of the draft Regulation says:

"1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:

(a) the offering of goods or services to such data subjects in the Union; or

(b) the monitoring of their behaviour.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law."

How this works in practice remains to be seen. The UK Commissioner has also expressed doubts as to how the Regulation's requirements can be readily enforced outside the EU.

Who will enforce the new rules?

The new rules will still be enforced by the independent data protection commissioners in each country and by the national courts. This is likely to lead to inconsistencies as in the present system. Fines vary across Europe for relatively similar incidents. In addition, the regulators in each country generally rely on registration fees to pay for their office. The Commission wants enforcement to be stepped up, but it remains to be seen who will pay for that, especially with the main regular source of income taken away. Fines are unlikely to be the answer, at least initially, as prosecutions are less likely with a prosecutor lacking resources. Given the current economic climate, it is unlikely most countries will prioritize strengthening data protection instead of other areas of spending like health and education. Already, the European Commission is threatening Hungary over its noncompliance with the existing data protection rules. Other countries have received less-well-publicized threats over underfunding of their regulatory authorities. Whether the Commission has the resources to pay for extra staff, or the ability to successfully force individual member states to prioritize spending in this area, is another question yet to be answered.

What about security breach?

Security breaches are the single-most common source of data investigations. The EU has had proposals to implement EU-wide laws in the past. Last May, a second EU Directive (the E-Privacy Directive (2009/136/EC)) introduced a requirement to give notifications following some security breaches. Telecoms companies and Internet Service Providers (ISPs) offering access to public networks are covered by the obligation. They have to notify regulators and, in some cases, those individuals whose personal data is affected. While the European Commission was keen that this need to notify was extended across all sectors, this proposal was resisted. However, some countries—notably Germany—introduced a general data breach notification requirement. This proposal is also not without its critics. There is credible evidence of security breach fatigue in the United States with too many consumers being told too much about relatively trivial breaches. The UK Information Commissioner in his response recognizes this risk, saying he considers that the reporting requirement should be restricted to serious breaches only. Many people who have experience of working through a breach would prefer the first 24 hours to be spent limiting the effects of the breach, helping to ensure it is not repeated and finding the people responsible. It would be unfortunate if companies were instead having to use that time to prepare reports to regulators and even more unfortunate if the perpetrators of crimes went unpunished, as the reporting obligation had prejudiced an investigation.

How long will the new rules take to implement?

The Commission's proposals will now be passed on to the European Parliament and EU member states (meeting in the Council of Ministers) for discussion. The European Parliament has clashed before with the European Commission over data protection issues, including the well-publicized disagreement over the transfer of airline data to the United States. It is fair to say that the Council of Ministers has a fairly full agenda currently with the euro crisis, and whether they will divert attention to the Regulation instead of those issues remains to be seen. Realistically, this process may take a year or more, especially given the fact that some of these proposals have previously been rejected. The Commission has said it then intends for a two-year implementation process, making the earliest realistic date sometime in 2015. While that may seem far into the future, since the law will apply to employees being hired now and contracts with a term beyond 2015, companies may want to start preparing now.

There are many uncertainties with the new proposals. It is apparent that changes will be made and there is likely to be widespread confusion between now and then. Companies should think now about how best to plan for those changes.

For Further Information

If you have any questions about this *Alert*, please contact Jonathan P. Armstrong in our London office, any member of the Corporate Practice Group or the attorney in the firm with whom you are regularly in contact.