Alerts and Updates

European Commission Issues New Data Protection Proposals

February 16, 2012

This Duane Morris Alert updates and expands on what we first reported on January 25, 2012, regarding the European Commission's new data protection proposals.

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 on 25 January. The aim of the proposals is 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 by Article 17 of the new Regulation. 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 and is likely to be highly controversial. 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 for organizations with more than 250 employees. This role exists (albeit on a quasi-voluntary basis) in Germany for organizations with more than 20 employees, 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.

- The tightening up of the definition of consent, which will need to be "explicit," *i.e.*, opt-in and not opt-out. Many businesses rely on the consent of consumers, employees and others they do business with to legitimize their data collection, processing and transfer. When the new Regulation is adopted, there is likely to be a higher bar and most organizations will want to look at moving to an opt-in now to help in their compliance efforts under the new rules and to avoid having to ask people for additional consents when the new rules come in. The burden of proof in establishing consent will be on the organization, not the individual.

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

- data mining and predictions based on that data

- health and epidemiological data

- CCTV and video data

- 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."

France's data protection authority, CNIL, says that it is firmly against the proposals, although they are in favor of some parts of it, including the right to be forgotten. CNIL believes the proposals will weaken their powers. They also object to the Regulation provision that would make the data protection authority in the

country where a business is headquartered the one in charge of data protection oversight and enforcement, rather than the DPA in the country where the data subject is based.

Germany has seen fierce debate as to whether the proposals are constitutional, despite many of the proposed changes being inspired by the current German data regime. The offices of the German Justice Minister, a prominent judge and at least two of the German data protection authorities (Germany has a state-level, not federal, system for privacy law enforcement) have expressed reservations. According to reports in Germany, the judge, Johannes Masing, said that he felt that the Regulation would encroach upon the German Constitution and remove the German Constitutional Court's jurisdiction over privacy and data protection issues. Masing said that the Regulation would render three decades of jurisprudence on data protection and informational self-determination in Germany obsolete.

The head of the Italian data protection authority (Garante per la Protezione dei Dati Personali), Francesco Pizzetti, has also expressed concerns at possible economic consequences as a result of the changes. Additionally, Pizzetti told the Italian Parliament that he was concerned about the greater centralization of data protection powers in Brussels.

In the U.S., the proposals have also not been without their critics. Jeffrey Rosen, Professor of Law at The George Washington University, said of the proposed right to be forgotten: "It represents the biggest threat to free speech on the Internet in the coming decade."

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 authorities 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. Whilst the European Commission was keen that this need to notify was extended across all sectors, this proposal was resisted. However, some countries—notably Germany and Austria—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. Currently the proposed threshold for reporting is lower. The proposal is that a breach would have to be reported to the regulator, even if only one person's information is involved and/or all of the information is already in the public domain. In addition—and unlike most U.S. states where similar laws already exist—there is no exception if the data is protected. Even if the information is subject to strong encryption or other security measures with the effect that it could never reasonably be accessed, a notification would still need to be made. For U.S. corporations, this could impose a significant burden as even with very few customers in the EU, the breach notification requirements could be triggered in Europe and effectively also in the U.S., despite U.S. law not requiring notification.

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.

Article 30 of the proposed new Regulation imposes a general obligation to keep data secure. Article 30(1) says:

"The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation."

In many respects, this language is little different from current data protection legislation in Europe—for example, Principle 7 of the UK's Data Protection Act 1998 has very similar language. What is different is the fact that the obligations to secure data are on the controller and the processor, rather than just on the

data controller alone. Article 30 also requires the controller and processor to evaluate the risks in their data handling and allows the Commission to *"adopt delegated acts"* to add to the detail which is required of controllers and processors *"including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default."* The Commission is also given the power to specify requirements for safeguarding personal data and preventing unauthorized access.

Article 31 contains the first new data breach notification requirement. The report should be made to the relevant data protection regulator *"without undue delay and, where feasible, not later than 24 hours after having become aware of [the breach]."* If a report is not made within 24 hours, then the report must be accompanied by a *"reasoned justification"* as to why the report is being delayed. The notification must:

1. Describe the nature of the breach, including the categories and number of data subjects affected.
2. Give the identity and contact details of the organization's data protection officer for more information.
3. Recommend measures to mitigate the possible adverse affects of the breach.
4. Describe the consequences of the breach.
5. Describe the measures proposed or taken to address the breach.

Again, the Commission in the Regulation wants the power to "adopt delegated acts" to further specify the criteria and requirements for the data breach notification requirement. This would include prescribing a standard notification format.

Article 32 deals with the need to communicate details of a breach to data subjects—the second new reporting requirement. Communication should be made to a data subject *"when the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject."* Again, it is envisaged that the notice to the data subject is in similar format to the notice sent to the regulator. Article 32(3) has a caveat however. It says:

"The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures will apply to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it."

Again, the Regulation seeks to reserve to the Commission the power to further specify the criteria under which a breach should be notified to data subjects and the format in which notice is given.

The right to be forgotten

In introducing the right to be forgotten, Commissioner Reding explained that the idea was to intervene to assist social media users who have posted comments or photographs which they later regretted. She said: *"If an individual no longer wants his personal data to be processed or stored by a data controller,*

and if there is no legitimate reason for keeping it, the data should be removed from their system." The right is contained in Article 17:

Right to be forgotten and to erasure

1. *"The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:*

   (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
   (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

   (c) the data subject objects to the processing of personal data pursuant to Article 19;

   the processing of the data does not comply with this Regulation for other reasons.

2. *Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.*
3. *The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:*

   (a) for exercising the right of freedom of expression in accordance with Article 80;
   (b) for reasons of public interest in the area of public health in accordance with Article 81;

   (c) for historical, statistical and scientific research purposes in accordance with Article 83;

   (d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject . . . ."

There are some limited exceptions to the right to be forgotten, for example, where the accuracy of the data is contested or where the data controller still needs the data "for purposes of proof." The "for the purposes of proof" exception only allows storage of the data—processing can only be undertaken on that data with the data subject's consent *"or for the protection of the rights of another natural or legal person or for an objective of public interest."* If consent is not obtained, the data controller must tell the data subject before this processing starts. There must also be a regular review of the continued need to hold and process the data.

The right is explained in paragraphs 53 and 54 of the preamble in the Regulation:

"Any person should have the right to have personal data concerning them rectified and a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation. In particular, data

subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. . . . To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party."

The right to be forgotten, however, poses a number of challenges not just to social media operators. All data controllers face penalties of up to 2 percent of their global income if they fail to remove photographs that people have posted in a moment of madness. Some may argue that the Commission's efforts would be better directed at educating individuals in proper social media use. [In the UK for example, Duane Morris has supported Nominet's "Know the Net" Campaign, which sought to do just that for social media users through a mixture of education, articles, outreach and an online self-assessment test (http://accidentaloutlaw.knowthenet.org.uk/).] Instead the Commission is proposing that any individual can exercise his or her right to be forgotten. This could have a chilling effect on law enforcement—for example, it is easy to envisage a criminal stalking somebody on Facebook and then asking Facebook to delete his postings. This wider right could play into the hands of those who wish to manage their reputation or distort an investigation into their past. Potentially more worryingly, criminals could also transfer their ill-gotten gains around the world and also exercise the right to be forgotten. Since at the time that they exercised the right there would be "no legitimate reason for keeping it" (for example to assist law enforcement), the trail could legitimately be erased. If the data controller keeps the data "for the purposes of proof" it can only store (and not process) the data once consent is withdrawn, and if any of the limited reasons apply to justify processing, it must notify the data subject before any processing commences. It is important to remember that the Commission's proposals as they stand are not limited to personal data that people themselves put onto social media sites, but instead they create a new right to delete personal data "relating to a data subject." How the right to be forgotten will work in practice seems to be deliberately vague. Reding said that it needed to *"stand for 30 years – it needs to be very clear but is precise enough that changes in the markets or public opinion can be maneuvered in the Regulation."*

How long will the new rules take to implement?

Contrary to some ill-informed reports, the new Regulations are not law now. 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 Commission itself feels that those negotiations should be complete this year. Some may view that is perhaps a little optimistic. 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 and given the opposition already in some

countries. 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.