Data Privacy: the European Commission pushes for total harmonization

(Translation of the article "*Protection des données personnelle: l'Europe ne veut voir qu'une seule tête*," Edition Multimedi@, February 13, 2012)

> ***Member States may challenge the Commission's proposal because it will render their national laws on privacy superfluous. Companies providing pan-European services will probably welcome the regulation, although it will impose significant new obligations on them, including the accountability principle.***

By Winston J. Maxwell, Hogan Lovells

The European Commission published on January 25, 2012 a proposed regulation for the protection of personal data in Europe. When adopted, the regulation would replace directive 95/46/CE, which has governed the protection of personal data in Europe for almost 17 years. The new regulation would not only replace the 1995 directive, it would supplant most national privacy laws. Unlike a directive, a regulation becomes immediately[1] operational in each Member State, much like a federal law would in the United States. By contrast, a directive does not have direct effect and must be transposed into national law by legislation adopted by the parliament of each Member State. The directive is a distinctly European form of legislation that affords each Member State flexibility to interpret the directive in light of national circumstances. A European regulation, on the other hand, requires no implementation. If the proposed European regulation on the protection of personal data is adopted, most provisions of France's 1978 law on the protection of personal data will become superfluous[2].

Imposing harmonization. The European Commission found that there are far too many differences in how Member States implemented the 1995 directive, leading to a lack of harmonization. The Commission is correct in its diagnosis. For example, when a company wishes to set up a pan-European product or procedure, the company must comply with the separate laws in the 27 Member States. Depending on the country in question, the company will either have to obtain an authorization, or file a declaration, or do nothing at all. Companies now find it difficult to establish pan-European compliance policies or launch pan-European services, and this results in high compliance costs and frustrates the objective of a single European market. Based on this diagnosis, the Commission proposes a potent remedy: a regulation instead of a directive. With the regulation, there will be only one data protection law in Europe. National privacy laws will to a large extent disappear.

The legal basis for a regulation. The Commission proposes to use article 16 of the Treaty on the Foundation of the European Union as the basis for adopting the regulation. Article 16 enables European institutions to adopt measures to guarantee the protection of privacy at a European level. However, article 16 does not specify what type of legal

---

[1] The proposed directive states that it will apply 24 months after its adoption.

[2] The law will continue to exist in order to govern the organization of the French data protection authority, the CNIL. Also, a national law will be necessary to implement the proposed directive on the protection of personal data in the context of law enforcement.

instrument may be used. The traditional legal instrument used in Europe is a directive, because it strikes a balance between European and national institutions and policies. This balance is imposed by the 2nd protocol to the European Treaty, which imposes on EU institutions the principles of subsidiarity and proportionality. The proposed regulation on privacy may well be criticized for violating these principles. Some Member States are likely to want to retain some of their national legislative prerogatives in connection with privacy, and may view the regulation as going too far in imposing harmonization.

Good news for pan-European operations. The creation of a single harmonized set of rules on privacy will be good news for companies that have pan-European operations. Companies will in theory have to comply with only one set of rules. The regulation will therefore simplify the compliance effort for many stakeholders. The other good news for companies is the elimination of the obligation to file notifications with national data protection authorities. When the regulation is adopted, notification and authorization procedures will largely disappear, except for personal data processing operations that present a certain level of risk for citizens. All other forms of processing will be free of bureaucratic filing obligations.

A shift from administrative filings to internal procedures. In exchange for less bureaucratic red tape, companies will have to implement stronger internal procedures to ensure compliance with the substantive rules of the regulation. Companies with over 250 employees will have to appoint a data protection officer; companies will have to maintain documentation to demonstrate their compliance with data protection obligations, and the documentation will be subject to audit; companies will have to conduct privacy impact assessments for data processing that raises particular risks for individuals; companies must implement "privacy by design" when they create new products, services or procedures. These new obligations are consistent with global privacy trends, which emphasize the accountability principle and privacy by design.

Non-European websites targeted. The proposed regulation modifies the rules on applicable law. Under the 1995 directive, some non-European websites are able to take the position that European privacy rules do not apply to them because the websites do not use "equipment" to process personal data in Europe. National data protection authorities, including the French CNIL, do not agree with this position; data protection authorities generally consider that the mere use of cookies by non-European websites is tantamount to the use of "equipment" in Europe and therefore brings websites under EU privacy laws. The proposed regulation would put an end to this debate, by subjecting any non-European company to European privacy rules to the extent the company offers goods or services to citizens in Europe, or monitors their behavior.

Individuals gain new rights. The proposed regulation would require companies to notify data breaches. This obligation already exists for telecom operators; the regulation would extend this obligation to all sectors. In France, companies would have to report data breaches to the CNIL, and to any data subject if the breach is likely to adversely affect the data subject's privacy. Data breach notifications have existed in the United States for a number of years. Given companies' experiences in notifying data breaches in the United States, the regulation's proposed 24 hour time period for reporting data breaches seems alarmingly short.

The proposed regulation would afford individuals a so-called "right to be forgotten." The "right to be forgotten" raises questions: First, how is this new right different from the rights that exist under the 1995 directive? The existing directive permits data subjects to have access to and require the deletion of personal data, and also requires that companies delete or anonymize all personal data as soon as they are no longer necessary for the original purpose for which they were collected. The "right to be forgotten" seems to be the same thing, with a new label. Second, the right to be forgotten can conflict with other fundamental rights, such as the right to free speech. An individual may want to hide part of his or her past, and in some cases (eg. a juvenile offense), this wish may be legitimate. In other cases, an individual's effort to hide his or her past will conflict with other individuals' right to free speech and free access to information. This is a tricky area where courts need to balance rights on a case-by-case basis. An across-the-board "right to be forgotten" seems too blunt an instrument.

Data portability. The regulation proposes to create a right to data portability. Telecommunications operators are familiar with "number portability:" the right for a consumer to retain his or her telephone number when switching operators. The Commission's proposal goes farther, by requiring that companies give all personal data back to individuals in a "structured and commonly used format." The reason for this obligation is apparently to permit individuals to move their data to a competing platform (eg. from Facebook to Google+) with minimal effort. The Commission appears to have a competition law objective in mind: to reduce switching costs. The data portability proposal may be questioned because the Commission did not conduct a market analysis to identify whether a market failure exists, and if it exists, whether *ex ante* regulatory measures are justified.

Data portability could potentially have far-reaching consequences beyond the Internet sector. For example, data portability could potentially require banks to return detailed customer data to their customers in a form that can be easily transferred to another competing bank. A measure such as this might be justified in a proposed measure to improve competition in the banking sector. But it is surprising to find such a far-reaching proposal in a regulation to protect privacy.