January 12, 2012

The text of a proposed new EU-wide regulation on data protection was made available in December 2011 in advance of formal publication this month.[1] The Explanatory Memorandum attached to the proposed General Data Protection Regulation (the "Proposed Regulation") states that it is the result of extensive consultations, which lasted for more than two years, by the European Commission ("Commission") with major stakeholders regarding the current data privacy framework. During these consultations, a large majority of stakeholders agreed that the general principles set out in the current Data Privacy Directive (officially, "Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data") remained valid, but there was a need to adapt that framework to respond to the rapid development of new technologies and increasing global harmonization.

Because the Data Privacy Directive required implementing law, each of the 27 EU Member States enacted different, and sometimes conflicting, data privacy laws that resulted in fragmentation of the rules on protection of personal data.[2] For this reason, the Commission is proposing the new rules be set forth in a Regulation, rather than a Directive. The direct applicability of a Regulation will reduce legal fragmentation and provide greater legal certainty by introducing a harmonized set of core rules that will apply to all EU Member States.

Reception to the Proposed Regulation, both inside and outside of the EU, has been mixed. Ronald Zink, chief operating officer for EU Affairs at Microsoft, noted that, "… [T]he EU data protection laws can be a beacon for the U.S. and around the world. They do a lot of things right."[3] But U.S. Internet companies are justifiably concerned that the Proposed Regulation will have substantial implications for them in at least seven key areas:

1. The Proposed Regulation expressly extends the jurisdictional reach of EU privacy laws to any data controller[4] that directs its processing activities to data of EU residents, no matter where the controller is located or the processing occurs.
2. In contrast to U.S. privacy law which regulates the online collection of personal data from children under the age of 13, the Proposed Regulation imposes rules on the collection of personal data from children under the age of 18.
3. The Proposed Regulation increases the obligations imposed on data controllers and processors, requiring them to be more proactive, to adopt internal controls that document processing operations, to make available upon request evidence of their data protection policies and procedures, to include statements on data policies in their annual reports, and to appoint data protection officers.
4. The Proposed Regulation strengthens individual rights to data privacy and creates new rights, including a right to be forgotten (permitting data subjects to request deletion of their personal data) and a right to data portability (permitting data subjects to a copy of their data to easily transfer to another service provider).
5. In addition to including provisions on data transfers similar to the current Data Privacy Directive, the Proposed Regulation makes it illegal to transfer data in response to an overseas court order without EC authorization.
6. The Proposed Regulation requires notification of data breaches under shorter time constraints and for broader types of data than required under security breach notification laws enacted under U.S. state laws.
7. The Proposed Regulation imposes heavy fines of up to 5% of a company's annual global revenue for serious

violations.

The Proposed Regulation is only a draft, and it is expected that it will take at least two years to finalize. Although it is unlikely that the Proposed Regulation will be submitted or enacted by the European Parliament in its current form, a number of the proposed changes to the current Data Privacy Directive reflect trends in privacy law worldwide and are likely to be implemented in some form in the final Regulation. The EU reform effort also comes at a pivotal point for U.S. privacy regulation. In March 2011, the Obama administration called on Congress to pass a "privacy bill of rights" for consumers and is finalizing specific policy recommendations, which are expected to be released soon. Although such action is unlikely to occur in an election year, the EU reform effort, coupled with the call to enact the first comprehensive federal privacy law in the United States, are developments that could make 2012 a pivotal year for privacy.[5]

1. The Proposed Regulation extends the jurisdictional reach of EU privacy laws.

As noted above, if there was ever any doubt as to whether the current Data Privacy Directive applied to organizations located outside of the EU, the Proposed Regulation expressly extends to any controller that directs its process activities to include personal data of EU residents, no matter where the controller is located or the processing occurs. The Proposed Regulation also requires all organizations subject to its jurisdiction to appoint a local representative, against whom enforcement action can be taken.[6]

2. The Proposed Regulation imposes new rules on the collection of data from children.

Although the Data Privacy Directive has no special rules for the collection of personal data from children, the Proposed Regulation defines "child" as anyone under the age of 18, provides that information provided to children must be in clear, plain language,[7] and requires parental consent for the collection of personal data or targeted marketing for children.[8] This contrasts with the U.S. Children's Online Privacy Protection Act (COPPA), which only requires parental consent for the collection of personal data for children under the age of 13, and may therefore conflict with current practices of companies subject to COPPA that allow children over 13 access to, and membership in, websites without first seeking parental consent.[9] In addition, the consent mechanism ultimately adopted by the Commission may not be consistent with COPPA mechanisms. If so, this may require companies to incur additional costs to comply with two sets of overlapping legal requirements for the collection of data from children.

3. The Proposed Regulation increases obligations on data controllers and processors.

The Proposed Regulation obligates data controllers to implement procedures and mechanisms to enable a data subject to exercise his or her rights, including providing a means for electronic requests, requiring response to a data subject's request within one month, and requiring the controller to provide the reasons for refusal, if a data subject's request is refused.[10] Not only are data controllers ultimately responsible for compliance with data protection rules, the proposed Regulation requires them to be more proactive and to take all those measures that are necessary to ensure that the data protection rules are complied with. This is referred to in the Proposed Regulation as the principle of "accountability." The Proposed Regulation also requires that data controllers be able to demonstrate that appropriate measures have been taken to ensure compliance with privacy requirements in the design of their systems ("data protection by design").[11]

Existing notification requirements in the Data Protection Directive are replaced by internal controls that document processing operations. Rather than having to comply with different regulatory filing requirements, the Proposed Regulation requires controllers to make available to data protection authorities, at their request, evidence demonstrating their data protection policies and procedures addressing their processing activities, including time periods relating to retention and erasure, as well as privacy by design and default mechanisms and privacy impact assessment.[12]

There are also new provisions relating to joint controllers, who are able to allocate responsibility for data breaches among themselves. Despite this allocation, however, each joint controller always remains jointly and severally liable to individuals unless the controller can demonstrate that it is not responsible for the data breach.[13]

Obligations on data processors are also increased. Every processing operation will need to be documented, and the documentation must be available to authorities on request. Annual reports will need to contain statements on policies and measures taken in relation to data processing. Under the Proposed Regulation, processors are obligated to provide assistance to a controller for data breaches or loss, and in relation to data at the end of the controller/processor relationship.

Data controllers and processors are required to implement appropriate technical and organizational 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. They are also required to conduct a data protection impact assessment prior to risky processing operations.[14] In certain cases, including where a controller or processor adopts contractual clauses for the transfer of personal data to a third country or an international organization or where a judgment of a court or administrative authority in a third country requests a controller or processor to disclose personal data, prior authorization from the supervisory authority will be required to ensure compliance.[15] The Proposed Regulation also encourages the development of codes of conduct to ensure compliance by including a provision for submission of such codes of conduct to the supervisory authority in a Member State for endorsement and by encouraging the establishment of data protection certification mechanisms, seals and marks.[16] Finally, all organizations employing more than 250 people will be required to appoint a data protection officer, whose core duties and responsibilities are set out in detail in the Proposed Regulation. The independent status of the data protection officer, with legal protection given to the officer, is a non-negotiable requirement.[17]

4. The Proposed Regulation strengthens individual rights to data privacy.

A number of disparate obligations implemented by Member States with respect to transparency have been combined into a single set of requirements that will apply to all personal data processing. Individuals have to be told the purposes of the processing and informed of their rights, what data is mandatory, the consequences of not providing data, the period during which the data will be retained, if the data will be exported, and if so, how it will be protected. Lawful processing of personal data remains based on (1) consent, (2) necessity for performance of contract, (3) legal requirement, (4) vital interests, (5) public interest, and (6) a controller's legitimate interests. The Proposed Regulation requires explicit permission from a data subject before a controller can collect data that alone or in combination with other data can be used to identify a person or create profiles about a person, including addresses, cookies and geo-data. Consent will not be valid where there is a "significant imbalance in the form of dependence between the position of the data subject and the controller," for example in the employment context. The Proposed Regulation also requires explicit consent for all forms of direct marketing, telemarketing and online (behavioral) marketing; explicit consent is not required for non-commercial purposes, such as charitable solicitations, recognized as being in the public interest so long as there is an ability to opt-out. This opt-in system is in conflict with the common practice of U.S. websites, which typically disclose the use of cookies, including for behavioral marketing, in their privacy policies and provide users with the ability to "opt-out" of such use. Finally, consent will not be valid if it cannot be withdrawn by the individual without detriment.

A new right to be forgotten is introduced in the Proposed Regulation.[18] The right to be forgotten is an extension of the existing right of objection and erasure and is intended in part to provide individuals with an opportunity to address youthful indiscretions by wiping the virtual slate clean.[19] As noted in a recent article, the potential for conflict between this right and existing U.S. laws has already emerged in a dispute between the Spanish government and Google. In January 2011 Google refused to comply with a request from the Spanish Data Protection Authority to remove approximately 90 links to newspaper articles and other public information that portrayed individual Spanish citizens in an unfavorable manner. Google argued that Spain's request inflicted serious harm of its freedom of speech and that removing the links would violate the objectivity of the Internet search. The case remains pending as of December 19, 2011.[20]

The Proposed Regulation also creates a right to data portability, which would allow individuals to transfer all of their data from one electronic provider to another (e.g., where an individual wants to move email accounts from one Internet based provider to another). Providers are also required to ensure that data is in a format that will facilitate the exercise of this right.[21]

5. The Proposed Regulation ensures high levels of protection for data transfers.

The Proposed Regulation provides that transfers to companies in foreign countries or to international organizations may only take place if the Commission determines that the level of protection is adequate, conditions equivalent to those set forth in the Proposed Regulation are complied with by the controller or processor, or other provisions of the Proposed Regulation (such as the approval of corporate rules) are complied with by the controller or processor.[22] Although these provisions are similar to the Data Privacy Directive, it is too early to determine what effect the Proposed Regulation will have on presently lawful bases for transfer of personal data outside the EU, such as the existing EU Standard Contractual Clauses, the U.S. Safe Harbor Framework, the list of countries approved by the Commission as providing adequate protection, or whether organizations with Binding Corporate Rules will have to amend them and seek re-authorization. As a result, it is possible that U.S. companies that are in compliance with the current EU Data Privacy Directive will be required to incur substantial additional costs to comply with the final regulation.

The Proposed Regulation would make it illegal to transfer data in response to legal requirements set outside the EU[23] Authorization would need to be obtained for use of non-Commission authorized standard contractual clauses or for transfers pursuant to an overseas court order. This may make it even more difficult for U.S. companies with European operations to comply with discovery requirements in U.S. litigation.

6. The Proposed Regulation requires prompt notification of data breaches.

The Proposed Regulation includes notification obligations that are similar to those currently required of providers of public communications services in the EU and broader than security breach notification laws that have been adopted in U.S. states. Unlike the U.S. where data breach notice laws only apply to unauthorized disclosure of data, the Proposed Regulation would potentially consider any data protection violation to be a breach. Also, while in the U.S. only sensitive data such as social security numbers and financial account numbers that can lead to identity theft are covered by breach notice laws, the Proposed Regulation would apply to breaches of not only the types of personal data that could result in identity theft but also breaches of any personal data that could result in physical harm, humiliation or damage to reputation. Data controllers, with full support of their processors, will be required to notify EU data protection authorities within 24 hours of a personal data breach.[24] In addition, if a processor processes personal data other than as instructed by a controller, the processor will be considered a controller with respect to that processing and will be subject to the rules on joint controllers set forth in Article 21. Controllers may also have to notify individuals if the breach is likely to have adversely affected them unless the controller is able to demonstrate to the data protection authority that it has implemented appropriate security measures.[25]

7. The Proposed Regulation imposes tough sanctions for data protection violations.

Based on the principle that penalties "must be effective, proportionate and dissuasive," the Proposed Regulation provides three tiers of sanctions for intentional or negligent violations of between 1%, 3% or 5% of an enterprise's annual worldwide turnover. Violations at the highest level include processing personal data, in particular sensitive personal data,[26] without a legal basis or otherwise in breach of relevant restrictions; not designating a representative; failing to notify regulators and, if required, data subjects, of personal data violations; and not designating a data protection officer when required to do so. Factors that will be taken into account in determining the remedy include the nature, gravity and duration of the violation, the degree of responsibility of the controller or processor and their previous compliance record; the technical and organizational measures and procedures they have

implemented; and the degree of cooperation with the regulator shown and steps taken to remedy the violation.

The growth in new technologies, mobile Internet devices, and web-user generated content has brought benefits to individuals, businesses and public authorities, but it has also created challenges for protection of personal data. The Proposed Regulation represents an attempt by the EU to strengthen individuals' rights to data privacy by ensuring that they understand what personal data is being collected, how it is being protected, what rights they have to control its collection and use, and when their personal data has been compromised. The Proposed Regulation also provides individuals and government authorities with substantial remedies against data collectors and processors who breach its terms. Although the Proposed Regulation is the first step in a lengthy process, many of the principles reflect legislative trends that are being discussed and enacted in a number of countries worldwide. As a result, U.S. companies will want to follow the progress of the Proposed Regulation as it progresses through the European Parliament.

NOTES

1. The draft of the Proposed Regulation is available **here**.
2. EU Justice Commissioner Viviane Reding estimates that the unnecessary hurdles created by these individual privacy rules cost companies 2.3 billion Euros, or $3.1 billion, a year as regulators in the 27 EU Member States apply their own rules. Eric Pfanner, *A Proposal for E.U.-Wide Data Protection Regulation,* N.Y. Times, Nov. 20, 2011 available **here**.
3. Id.
4. A "controller" is defined as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data." Proposed Regulation, Article 3, §5.
5. Alexei Alexis, *EU Rule Would have "Serious" Global Impact; Election Year Congress Won't Act, Privacy Forum Says,* 11 PVLR 60, January 9, 2012.
6. Proposed Regulation, Article 19 §22(1).
7. Proposed Regulation, Article 9 §2.
8. Proposed Regulation, Article 7 §6.
9. U.S. consumer organizations like the Electronic Privacy Information Center have urged Congress to extend COPPA protections to 13- to 18-year olds. *That Facebook Friend Might Be 10 Years Old, and Other Troubling News,* Consumer Reports Magazine, June 2011, available **here**.
10. Proposed Regulation, Article 10.
11. Proposed Regulation, Article 20.
12. Proposed Regulation, Article 25.
13. Proposed Regulation, Article 21.
14. Proposed Regulation, Article 30.
15. Proposed Regulation, Article 31.
16. Proposed Regulation, Articles 35-36.
17. Proposed Regulation, Articles 32-34.
18. In a memorandum explaining its proposals on the right to be forgotten, the EC characterized the right as "the right of individuals to have their data no longer processed and deleted when [it is] no longer deleted for legitimate purposes. An 11/11/10 E.U. press release explained: "People should be able to give their

informed consent to the processing of their personal data, for example when surfing online, and should have the 'right to be forgotten' when their data is no longer needed or they want their data to be deleted." Axel Spies, *Reform of the E.U. Data Protection Directive: "Right to be Forgotten"—What Should be Forgotten and How?,* Privacy and Security Law Report, Dec. 21, 2011, available **here**.

19. The Proposed Regulation states, "This right shall apply especially in relation to personal data which are made available by the data subject while he or she was a child." Proposed Regulation, 15 §1.
20. Spies, *supra* note xviii.
21. Proposed Regulation, Article 16.
22. Proposed Regulation, Article 37.
23. Proposed Regulation, Article 42.
24. There is a new definition of "personal data breach," which covers all types of security breaches, including when data is in transit, being stored or otherwise processed. Proposed Regulation, Article 28.
25. Proposed Regulation, Article 29.
26. Article 8 of the Proposed Regulation sets forth special rules that restrict (subject to exceptions enumerated therein) processing of "special categories of personal data," which it describes as personal data revealing "race or ethnic origin, political openness, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or offenses or criminal convictions or related security measures."

Key Contacts

Adam Ruttenberg Washington, DC	aruttenberg@cooley.com +1 202 842 7804