What the Proposed EU Data Protection Regulation Means for Cloud Users

CSA Legal Information Center Sponsored Research

INTRODUCTION

The Cloud Security Alliance is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. CSA sets the pace as the industry leader in research, best practices and certification for the trusted cloud ecosystem.

The CSA Legal Information Center is an expert-led community resource for global legal issues impacting cloud computing. Our mission is to provide unbiased information about the applicability of existing laws and also identify laws that are being impacted by technology trends and may require modification. The CSA Legal Information Center includes whitepapers, webinars, an advice column and in-person events.

The CSA Legal Information Center is located at: https://cloudsecurityalliance.org/research/clic/

The CSA Legal Information Center is supported by our founding sponsor and corporate member Box. Founded in 2005, Box provides a secure content sharing platform that both users and IT love and adopt. Content on Box can be shared internally and externally, accessed through iPad, iPhone, Android, TouchPad and PlayBook applications, and extended to partner applications such as Google Apps, NetSuite and Salesforce. Headquartered in Palo Alto, CA, Box is a privately held company and is backed by venture capital firms Andreessen Horowitz, Draper Fisher Jurvetson, Emergence Capital Partners, Meritech Capital Partners, Scale Venture Partners, and U.S. Venture Partners. To learn more about Box, please visit www.box.com.

Author Acknowledgment

Francoise Gilbert, JD, CIPP/US, focuses her legal practice on information privacy and security, cloud computing, and data governance. She was listed as one of the country's top legal advisors on privacy matters in a recent industry survey and, for several years, has been recognized by Chambers, Best Lawyers, as leading lawyer in the field of information privacy and security. For the past two years, Ethisphere has identified her as "an attorney who matters" in the field of information privacy and security.

Gilbert is the author and editor of the two-volume treatise Global Privacy & Security Law (3,000 pages; Aspen Publishers, Wolters Kluwer Law and Business) (www.globalprivacybook.com), which analyzes the data protection laws of 65 countries on all continents.

She is the managing attorney of the IT Law Group (www.itlawgroup.com) and serves as the general counsel of the Cloud Security Alliance. She also keeps a blog on domestic and international data privacy and security issues (www.francoisegilbert.com). (650) 804-1235 fgilbert@itlawgroup.com

What the Proposed EU Data Protection Regulation Means for Cloud Users

Francoise Gilbert JD, CIPP/US

The recently published draft of the proposed European Union data protection regulation, which is intended to replace Directive 95/46/EC[1] in 2014, provides a preview of how the European Commission intends to reshape the rules that govern the protection of personal information in the European Economic Area (EEA). If the final version of the regulation (expected to be released during the first quarter of 2012) is substantially similar to the currently available draft, there will be significant improvements in the new regime: more clarity, less complexity, less administrative burdens. However, there will also be additional obligations and responsibilities for companies that collect or process personal data. This article will focus on some of the provisions of the proposed EU data protection regulation[2] and evaluate their potential effect on cloud computing users and service providers.

Less Discrepancies Among the Members of the EEA

The most significant change from the current data protection framework of the EEA is that this new document will be in the form of a "regulation" rather than a "directive." This means it will be directly applicable within the Member States as the national law of each country.

This is not the case in the current regime. Directive 95/46/EC, commonly known as the "Data Protection Directive," is not the national law of any of the Member States. It had to be transposed or implemented into the national laws of the EEA Member States. As a result, each country adopted its own interpretation of the principles set forth in the directive, which created a patchwork that lacked the expected uniformity and consistency.

With the new EU data protection regulation, there will be one single rule: The countries will not have the freedom to make choices. As soon as the regulation is passed, each of its provisions will become part of the national legal system of each EEA Member State, "as is." The wording will not be changed. Concurrently, the national laws of the Member States regarding the same subject matter will be superseded.

In other words, there will be one single law throughout the EEA. This uniformity should be welcomed by companies, as they will be assured to be subject to the same obligations everywhere in the European Economic Area, no matter where they are operating.

However, ***this apparent uniformity is likely to be illusory***.

- The proposed Regulation offers Member States many opportunities to make changes, set exception, ignore certain provisions, etc.

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

- The new Regulation would supersede only the Member States' national data protection laws that previously implemented the 1995 Directive on Data Protection. Each country has a much more complex web of national laws that will remain untouched. For example, employment laws that protect individuals in the work place, or healthcare laws that govern the protection of health data.

Security requirements when engaging a cloud provider

Article 26 of the proposed European Union data protection regulation, if adopted with its current wording, will be one of the key provisions affecting cloud-computing services. This provision expands on the wording of the current Article 16 of Directive 95/46/EC, and is more specific and more comprehensive.

First, a company (data controller) that elects to process its data in the cloud will be required to choose a service provider that provides sufficient guarantees to implement appropriate technical and organizational measures in such a way that the processing meets the requirement of the data protection regulation and ensures the protection of the rights of the individuals. In other words, the data controller (cloud service client) must ensure not only that the data processor (cloud service provider) uses security measures, but also that the processing conducted, and the security measures used, by the service provider meet the regulation. This very specific requirement could be problematic since cloud service providers have generally been reluctant to share or disclose the nature of the security measures they use, or the way they process the data in their custody.

Several other requirements in Article 26 of the proposed regulation would go well beyond the current rules. For example, the contract between the cloud service client and cloud service provider will have to prohibit the provider from retaining the services of a third party without the permission of the client (Art. 26(2)(d)). In general, cloud service providers have refused to agree to this type of clause. Thus, difficult negotiations should be expected.

The contract will also have to require the data processor to hand over all data to the data controller after the termination of the contract. (Art. 26(2)(g)). In addition, the contract will have to require the data processor to make available to the data controller and the country's Data Protection Supervisory Authority all information necessary to control compliance with the data processor's obligations. While the provision makes sense from a data protection standpoint, it is likely to create an administrative burden on cloud service providers, which may result in an increase in the fees for their services.

Data security and risk assessment requirements

The security provisions under Articles 30 of the proposed data protection regulation are also much more extensive than previously under Directive 95/46/EC and more stringent than what is usually found under U.S. law.

Article 30(1) would require both data controllers and data processors to use security measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be processed. The equivalent provision in Article 17 of Directive 95/46/EC merely requires the use of "appropriate security measures." Under the proposed regulation, the security measures would have to be adapted to the specific risks represented by the processing and the nature of the personal data to be protected, and would have to take into account the state of the art and cost of implementation. Further, Article 30(2) would require both the data controller and the data processor to conduct a risk assessment.

While these obligations are consistent with current best practices and industry standards, they are likely to create a burden for cloud computing services, unless business models change. Indeed, the current cloud computing business

model is usually that of a "one-size-fits-all." In many arrangements, such as Infrastructure as a Service (IaaS) services, the service provider does not know -- or want to know -- the nature of the data hosted by the service. Thus, conducting a risk assessment and identifying the specific measures that are adapted to the category of data to be processed may cause significant delays and additional costs.

On the other hand, SaaS service providers, which usually target a specific market or specific categories of data, may be able to take advantage of the new provisions and tout their ability to provide tailor-made, targeted security measures or risk assessment processes because their services are usually directed at specific types of data and they can more easily comply with the risk assessment and tailored security measure requirements.

Breach notification requirements

Article 31 and 32 of the proposed European Union data protection regulation would introduce a notification obligation in case of a breach of security, a concept most U.S. companies are now very familiar. The major difference with U.S. law, however, is that what constitutes a "personal data breach" is much broader under the draft regulation.

The regulation would define personal data breach as any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. This definition is very broad. Keep in mind that the definition of personal data in the EEA includes "any information relating to a data subject." This really means ***any*** data, and not just Social Security numbers, credit card information or health information, as is the case under most U.S. state security breach laws. Thus, the loss or unauthorized modification of an email address or a phone number would constitute a personal data breach.

The rules that would apply to a personal data breach are also much more stringent than in any of the more than 47 U.S. breach disclosure laws. Under the new regulation, in the event of a personal data breach, the data controller (in most cases, the cloud service client) would have to disclose the occurrence of the breach to the country's supervisory authority ***within 24 hours, if feasible***. Further, if the breach is "likely to adversely affect the protection of the personal data or the privacy of the data subject," Article 32 of the draft regulation would require that the data controller also notify the data subjects without undue delay after having notified the supervisory authority. This requirement is also much more stringent than current U.S. laws.

Unless subsequent implementing documents temper and clarify the proposed requirement, these provisions are likely to cause a deluge of breach notices, and to unnecessarily trouble and confuse the average citizen. This confusion, in turn, could cause unnecessary additional expenses for companies who will have to arrange for call centers, support, and communications to calm or control the anxiety that the disclosures may cause.

What's next

The final version of the new European Union data protection regulation is expected to be finalized in 2013 and to come into force two years later, approximately in mid to late 2015 or 2016. Since the drafting of this proposed regulation has been in process for more than a year, the current document is probably very close to a final draft, and thus, it is unlikely the final draft will drastically differ from the current document. American cloud service providers and users of cloud services should prepare and budget for a new, stricter, and more complex era of data protection in Europe with more requirements and more stringent provisions.

This article was first published by TechTarget in January 2012