Akin Gump
STRAUSS HAUER & FELD LLP

Cybersecurity, Privacy & Data Protection Alert

December 21, 2015

If you read one thing…

- The new EU-wide legal framework will have an extremely significant impact on how businesses collect, store, transfer and use data.
- The Data Protection Authorities at the national level (and below, where applicable) will all apply and interpret the same law, thereby harmonizing data protection rules across the EU to the benefit of the increasing number of cross-border businesses.
- Although the regulation won't become effective until two years after the approvals, companies should engage now to begin devising a comprehensive compliance program, including data mapping, hiring privacy compliance staff, resource allocation planning, budgeting, testing and implementing, and also analyzing potentially significant changes in business practices.

The EU General Data Protection Regulation

On December 15, 2015, European Union ("**EU**") politicians and officials reached a political agreement on a new EU-wide legal framework to govern data sharing and collection and related consumer privacy rights. It is called the General Data Protection Regulation (the "**Regulation**") and it will have an extremely significant impact on how businesses collect, store, transfer and use data. The Regulation consists of a rule package of more than 200 pages and represents the biggest update to EU privacy law in two decades. Although the text of the agreement has yet to be finalized or published, and refinements are possible until final approval is given by the European Parliament (the "**Parliament**") and the Council of the EU (the "**Council**"), the version that is now publicly available is likely to be very close to what is eventually published. After the approvals, the Regulation will be translated and published in 24 languages, likely around May, and will become effective two years after that. While companies may be tempted to sit back until just before the Regulation becomes effective, ensuring timely compliance will require a substantial lead-in time in order to allow for data mapping, hiring privacy compliance staff, resource allocation planning, budgeting, testing and implementing, and also analyzing potentially significant changes in business practices.

Background

In January 2012, the European Commission (the "**EC**") first proposed a new data protection framework to replace the EU Data Protective Directive of 1995 (the "**Directive**"). As a Regulation rather than a Directive, the new law will directly apply to and bind the 28 EU Member States, and not require national

adoption. The Data Protection Authorities ("**DPAs**") at the national level (and below, where applicable) will all apply and interpret the same law, thereby harmonizing data protection rules across the EU to the benefit of the increasing number of cross-border businesses. Up until now, there has been a patchwork quilt of varying privacy rules, from the stricter, more formalistic jurisdictions (led by Germany), to the more principles-based and flexible jurisdictions (including the United Kingdom).

Following numerous amendments to the EC draft proposed by the Parliament in 2014, it was left to the Council – which shares legislative powers with the Parliament – to put its proposal on the table. Next came the Trialogue negotiations, during which the EC, the Parliament and the Council negotiated their draft proposals. Finally, on December 15, 2015, the Parliament and the Council announced a political agreement with respect to a consolidated text of the Regulation. The Regulation will replace the Directive in its entirety.

Key Rules Under the Regulation

New Requirements for Business

- *Expanded scope.* The Regulation applies to any controller or processor of EU citizen data, regardless of where the controller or processor is headquartered or keeps its servers. This means that virtually any business that offers its products or services to EU consumers will fall within scope. In particular, the Regulation will apply to the online activities of non-EU companies that offer goods or services to, or monitor the behavior of, EU residents, including third-party technology service providers who may not have been formally covered by rules in many Member States. This is likely to have a major impact on the cloud industry. For example, cloud-based processing performed outside of the EU for an EU-based company is covered by the Regulation.
- *Personal data.* The Regulation expands the Directive's definition of personal data, defining it as "any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person." In addition, two new categories of data, genetic and biometric data, join the prior list of "sensitive" or "special" personal data: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life and sexual orientation.
- *Consent.* As it was under the Directive, consent is one of several possible bases for processing personal data. Consent must be freely given, specific and informed, and demonstrated by a "clear affirmative action by the data subject." There are also several new limitations on consent, including that consumers cannot be asked to agree to any unfair contract terms in exchange for their consent. Moreover, consent will not be deemed valid in the context of any contract if the data subject is required to give consent to use his or her personal data that is unnecessary for performance of the contract or service.

- *International data transfers.* The Regulation will maintain the general prohibition of data transfers to non-EU countries that are not officially recognized as "adequate" by the EU, including the United States, but stricter conditions will apply for obtaining such "adequate" status. The *Schrems* decision of the Court of Justice of the EU recently torpedoed the Safe Harbor agreement between the United States and EU as one available method for ensuring U.S. legal adequacy (and may have implications for other methods) and those who rely on it have been told that enforcement against them is unlikely before January 31, 2016. Observers are hopeful that by that time there might be a new agreement in place between the U.S. government and the EC to replace Safe Harbor.
- *Data protection officer.* Many companies, including all public bodies processing data, all companies where data processing is a "core activity," and all companies where sensitive data is processed on a "large scale" will now be required to appoint a data protection officer. Data protection officers will be more akin to in-house compliance officers, although there may also be an opportunity to outsource this function; a high level of independence will be key.
- *Breach notification.* The Regulation will require companies to notify regulators of any data breach that creates significant risk for the data subjects involved within 72 hours of discovery of the breach.
- *Higher fines.* The maximum fines for violations of data protection law will increase dramatically under the Regulation, with DPAs able to impose fines for noncompliance up to 4% of a company's global revenue in some instances. European policymakers had been concerned that the lighter penalties previously associated with privacy violations were inadequate and an effort was made to more closely follow the model of EU competition law, which can result in penalties up to 10% of a company's global revenues.
- *More centralized enforcement.* The Regulation will allow businesses to deal primarily with a single national privacy regulator in Europe. Although EU officials have used the term "one-stop-shop," in practice this promises to be more complex. Companies that operate in multiple EU countries may need to interact with DPAs in various Member States prior to going before a pan-European board of regulators.

New Individual Rights

The Regulation creates or clarifies rights for individuals to control their personal data. Among other things, the Regulation will codify that individuals have a "right to be forgotten" and create a right to easily transfer personal data from one service or product to another ("right to data portability"). The Regulation also boosts the digital age of consent from 13 to 16 years old. This last development may raise challenging issues for companies in light of the substantially increased number of consents they may need to obtain, from an age group with very active online lives, their own money and possibly lighter parental supervision.

Next Steps

The final text of the Regulation will be submitted for a formal vote of the Parliament and the Council early next year. The Regulation will take effect two years after its adoption – *i.e.*, likely in the first half of 2018. Given the complexity of the Regulation, the scope of its impact on the way multinational corporations collect, store, transfer and use data, and the lead times on IT projects, we are advising clients to engage

now to begin devising a comprehensive compliance program, including a road map and implementation timeline. Akin Gump's privacy and data protection experts are available to start the compliance conversation and data-mapping process to prepare you for these upcoming changes. Stay tuned for Akin Gump's privacy and data protection event in late Winter/early Spring, to be held in Washington, D.C.

Contact Information

If you have any questions regarding this alert, please contact:

Davina Garrod
davina.garrod@akingump.com
+44 20.7661.5480 | London

Natasha G. Kohne
nkohne@akingump.com
+971 2.406.8520 | Abu Dhabi
+1 415.765.9500 | San Francisco*

Michelle A. Reed
mreed@akingump.com
+1 214.969.2713 | Dallas

David S. Turetsky
dturetsky@akingump.com
+1 202.887.4074 | Washington, D.C.

Jo-Ellyn Sakowitz Klein
jsklein@akingump.com
+1 202.887.4220 | Washington, D.C.

Isabelle R. Gold
igold@akingump.com
+1 212.872.7482 | New York

*Licensed to practice for 15 years in New York. Practicing in California under the supervision of the partners of Akin Gump Strauss Hauer & Feld LLP. Application for admission to the California Bar pending.