WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

Agreement on EU General Data Protection Regulation Sets the Stage for New Obligations and Higher Penalties for Noncompliance

December 17, 2015

AUTHORS

Daniel K. Alvarez | **Dr. Christian Rolf**

Overview

On December 15, 2015, the European Commission ("EC") announced an agreement on the final details of the European Union's ("EU's") Data Protection Reform effort, known as the General Data Protection Regulation ("GDPR"). This agreement is the culmination of a process that began in January 2012 to update and replace existing EU data protection laws, and we expect that it will have significant repercussions for all businesses that operate or have customers in the EU. Final approvals by the European Parliament and the 28 EU national governments, as well as the final text of the new rules, are expected in early 2016, and the rules are expected to go into effect two years after their final approval, (*i.e.*, early 2018).

How We Got Here

These new rules represent a significant change in EU data protection law. For many years, the concept of "European Data Protection Law" has been more accurately defined as an EU Directive – a framework of data protection requirements that each member state converted into state-level laws. This approach resulted in a patchwork of 28 national data privacy laws that, while ostensibly grounded in the same set of requirements, often led to significant practical differences for both

businesses and consumers. The EC recognized the shortcomings of this approach, and the GDPR, unlike an EU Directive, will be one binding law effective in all EU member states.

Where We Are

We do not yet know exactly how the compromise will be translated into the actual wording of the GDPR. However, based on early reports and the EC's own press release, we believe that the agreement includes significant substantive changes to privacy and data security law in the EU. Most importantly, we believe the practical effect of the new rules is to create significant new obligations, as well as potential liability for failing to fulfill those obligations, for companies operating or having customers in the EU. Some examples include:

- Penalties for Noncompliance. Maximum penalties for violations can reach up to *four percent of the company's global revenues*.
- Breach Notification. Very short deadline – 72 hours after discovery of a data breach – to inform national regulators of the breach, unless the company can demonstrate that the breach "is unlikely to result in a risk for the rights and freedoms of individuals."
- User Control. Enhanced obligations to provide users with control over their data, including the right to correct any inaccurate data and the enshrinement and clarification of the so-called right to be forgotten.
- Notice. Enhanced transparency obligations to provide users more information about what data a company is collecting and how that data is being used.

Other notable provisions of the new rules include:

- Risk-Based Obligations. Companies may tailor their data security measures to match the risk of data breach and resulting harm to users, rather than conforming to a one-size-fits-all requirement.
- Pseudonymized Data. Pseudonymized data is still considered personal data, but the new rules recognize pseudonymization as a highly recommended risk-reduction technique.
- Children's Data. The age of consent is 16, though reports indicate that individual EU nations will be free to set a lower age limit, to be no lower than 13.

While the rules include provisions regarding the transfer of data to third countries, they do not tackle the issues raised by the recent invalidation of the EU-U.S. Safe Harbor framework by the European Court of Justice. We described the issues raised by that decision in our October 7, 2015 Client Memorandum, and our perspective has not changed: unless and until EU and U.S. authorities are able to update the Safe Harbor framework, companies seeking to transfer personal data

between an EU member state and the United States must carefully consider and analyze other potential alternatives discussed in our October 7, 2015 Memo. We will update you if that changes.

Where We Go From Here

As noted, the next steps will be for the European Parliament and the EU nations to give their formal approval to the agreement. We expect the final text to be released shortly thereafter, and that companies will then have two years to make any changes to their business practices to comply with the new rules.

We will continue to update you as this process moves forward. In the meanwhile, we encourage you to call with any questions you may have.

If you have any questions regarding this memorandum, please contact Daniel K. Alvarez (202-303-1125; dalvarez@willkie.com), Dr. Christian Rolf (+49-69-79302-151, crolf@willkie.com) or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

December 17, 2015