New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 254—NO. 69
TUESDAY, OCTOBER 8, 2015

Outside Counsel

Expert Analysis

U.S. Investigations And EU Data Privacy Regime

As U.S. regulatory investigations become increasingly global, the EU data protection laws and the restrictions they impose present major challenges for companies that want to cooperate with authorities by transferring requested EU data to the United States.

Recent developments in both jurisdictions, such as the Google Spain Decision of the European Court of Justice,[1] the opinion of the Advocate General Bot in the Schrems Case,[2] and the Southern District of New York's Microsoft-Ireland decision[3] intensify the inherent conflict between the strict EU data protection rules and the extraterritorial reach of U.S. investigations. Also, by the end of 2015, a new General Data Protection Regulation (GDPR) is expected to change the EU data protection landscape and, in many cases, result in even more stringent laws while imposing heftier penalties for non-compliance.

Thus, it is crucial for companies to understand the data protection laws and the options for cooperating with authorities while also complying with the applicable laws.

This article details the current landscape of EU data privacy law in the context of U.S. regulatory investigations, while also touching upon the changes that may ensue when the new GDPR is adopted.

Data Privacy: EU vs. U.S.

Under EU law, the protection of personal data constitutes a fundamental right with constitutional value.[4] As a result, the EU Data Protection Directive (DPD) generally prohibits the transfer of personal data[5] to countries that do not offer an equivalent level of protection as the transferring country. Moreover, the DPD only provides for very few exemptions from its restrictions. As the DPD is only binding as to the result to be achieved and leaves to the member states the choice of form and methods, some member states, such as Germany, chose to adopt even stricter rules than those provided by the DPD.

By **Anahita Thoms**

As compared to the EU's DPD, the U.S. is considered a country that does not offer an equivalent level of data protection and, as a result, a transfer from the EU to the U.S. falls under the DPD's general prohibition.

By the end of 2015, a new General Data Protection Regulation is expected to change the EU data protection landscape and, in many cases, result in even more stringent laws while imposing heftier penalties for non-compliance.

In light of this, the EU data privacy laws often present challenges to U.S. companies, as investigations by U.S. authorities are becoming increasingly global and often implicate EU data.

Companies are often willing to cooperate with regulatory requests to provide data, but their ability to do so is limited by their obligation to comply with EU data protection rules. Moreover, a violation of the EU data protection laws can have severe consequences. Under the DPD, a breach of data protection laws can cause regulatory and even criminal penalties under certain circumstances, and breaches are also significant reputational risks. If the draft for a new GDPR is adopted, fines up to 5 percent of a company's worldwide turnover up to 100 million € could be imposed by EU regulators.

As a result, companies have to thoroughly consider what limits are set out by the EU data protection rules when evaluating how to cooperate with U.S. authorities in cross-border investigations and inquiries.

Current Framework

Although the DPD provides for some exemptions that allow a transfer to countries with inadequate levels of protection, these exemptions are often difficult to invoke.

The DPD allows the transfer of data that is "necessary or legally required on important public interest grounds." This provision is often interpreted as only covering binding obligations imposed by laws of the EU or of a member state, not by a third country. Therefore, the "request" of a U.S. authority generally does not constitute a "legal requirement" under the DPD. Moreover, the term "public interest" is interpreted to be limited to an interest of the EU or its member states, and thus a "request" of a U.S. authority would generally not fall within the scope of this exemption.

Another exemption under the DPD allows for the provision of data necessary for the establishment, exercise or defense of legal claims. This provision's scope is often interpreted as being limited to court proceedings and does not apply to the request of an authority in an isolated regulatory proceeding. Some member states, such as Germany, expressly provide for a limitation of this exemption to court proceedings. The rationale behind the exemption is a certain trust in the procedural rules of court proceedings, which are expected to secure a sufficient level of data protection.

A possibility for companies to justify a transfer of EU data to a U.S. authority would be the unambiguous consent of the data subject. However, consents are only valid if given freely, specific and informed. Especially with regard to employee

ANAHITA THOMS *is counsel at Freshfields Bruckhaus Deringer US.* JONATHAN ELSNER, *an associate at the firm, assisted in the preparation of this article.*

data, there is a risk that the consent might not be deemed to be freely given due to the pressures employees may feel to sign a consent form presented by an employer.[6]

Even if a company falls under an exemption, it must also comply with the general DPD restrictions. The transfer of data is only legitimate if necessary and proportional to the specific purpose of the request. Therefore, the data controller (e.g., the company) must only provide documents to the regulator that are relevant for the purpose of the investigation. Furthermore, a transfer must be justified by a legitimate interest of the data controller. Whether a legitimate interest exists requires balancing the interest of the company and the effect a transfer could have on the rights of the data subject, taking into account the nature of the data. In general, the disclosure of data to an authority in the context of an investigation serves a legitimate interest of the company.

Practical Solutions

Aside from the above-mentioned exemptions, other possibilities do exist for providing data to U.S. authorities, such as entering into a data transfer agreement (DTA) with the U.S. authority. However, U.S. authorities are often unwilling to agree to the terms that are necessary to make a DTA legally sufficient.[7]

Additionally, if it is clear that a review of EU data within the EU is permissible under EU laws but a transfer of EU data to the U.S. will violate EU laws, certain U.S. regulators may be willing to conduct a review within the EU either at a neutral site or onsite at a company's office.

Utilizing a regulator-to-regulator channel is another option. This entails an official request by a U.S. authority of the EU regulator for judicial assistance. This procedure may, however, be time-consuming and less than ideal to the U.S. authority requesting the data.

Also, an option that always remains is anonymizing the documents by redacting them in a way that it is not possible for the recipient to determine the identity of the person the data is relating to. This option, however, is likely to be time-consuming and expensive. Furthermore, U.S. authorities may (and often do) want to know the names of the relevant individuals in their investigations. Regulators may, however, be more amenable with the prospect of anonymizing documents while also using pseudonyms to replace the anonymized names (e.g., "Employee 1," Employee 2," etc.).

If companies are unsure whether a particular transfer of EU data is compliant with the EU data protection laws, another option is reaching out to the relevant data protection authority on a no-names basis for guidance. Data protection authorities are indeed often willing to provide guidance in these scenarios.

The new GDPR

There might be some clarification to what extent companies will be able to cooperate with requests of authorities of non-EU states after the adoption of the new GDPR. However, the contents of the pending GDPR are still unclear.

The positions taken in the drafting of the new GDPR—with the EU Council and the European Commission on one end of the spectrum and the European Parliament (EP) on the other—are very controversial. The original draft of the new GDPR provided for an additional exemption that would allow a transfer of data to a third country if there was a legitimate interest of the controller or processor. This would clearly broaden the possibilities to justify a data transfer to third countries—such as the U.S.—in comparison to the DPD.

> The EU Data Protection Directive generally prohibits the transfer of personal data to countries that do not offer an equivalent level of protection as the transferring country. Moreover, the DPD only provides for very few exemptions from its restrictions.

The EP rejected this attempt and additionally proposed to introduce a new provision that would generally prohibit the data transfer following the request of a third party without prior authorization of a supervisory authority. Such an approach would be even stricter than the existing regime. As a final adoption of the GDPR requires the approval of both the EU Council and the EP, the outcome is not predictable. The latest negotiations between the EU institutions in July 2015 did not lead to conclusions on these challenging questions.

Conclusion

The EU data privacy regime often presents various challenges to cooperating with cross-border U.S. regulatory investigations.[8] While certain exemptions may in rare instances allow for the delivery of EU data to U.S. authorities, there are often practical solutions that will allow for the cooperation with U.S. authorities.

However, aside from the expected adoption of the GDPR in late 2015, there are other expected developments that may further reshape the interplay between the EU data privacy rules and U.S. regulatory investigations. For example, the Southern District of New York's recent Microsoft-Ireland decision—for which the U.S. Court of Appeals for the Second Circuit is currently hearing an appeal—unveiled the potential extraterritorial reach of U.S. investigation powers and raised further questions with regard to compliance with data protection laws. Indeed, in the Southern District's Microsoft-Ireland decision, the court held that the U.S. Department of Justice could compel Microsoft—a domestic company—to produce data stored overseas.

To navigate this complex interplay between the EU data privacy regime and U.S. cross-border regulatory investigations, it is essential for companies subject to cross-border investigations to work closely with their in-house data protection officers and legal/compliance departments. Doing so will often allow companies to reach solutions that are both cooperative with regulatory inquiries but also compliant with the EU data privacy regime.

1. Decision of the European Court of Justice of 13 May 2014, Case C-131/12—*Google Spain v AEPD*. In this case, a Spanish resident lodged a complaint against Google Spain and Google Inc. for listing the complainant's name in search engine results. The ECJ found that each data subject has a right to request that the information relating to him should no longer be displayed if a search of his name is performed, and that operators of search engines, such as Google, are obliged to remove links to web pages that contain information relating to that data subject.

2. OPINION OF ADVOCATE GENERAL BOT delivered on 23 September 2015, Case C?362/14—Maximillian Schrems/ Data Protection Commissioner.

3. *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 15 F.Supp.3d 466 (S.D.N.Y. 2014).

4. Article 8 of the EU Charter of Fundamental rights emphasizes that "everyone has the right to the protection of personal data concerning him or her."

5. Personal data is defined as any information relating to an identified or identifiable natural person.

6. Under a very strict interpretation, it is even necessary to specify the recipient and the country the data will be transferred to. Whether it is feasible to meet the conditions depends on the circumstances and has to be assessed on a case-by-case basis.

7. The Safe Harbor Framework is often discussed as an option in transferring EU data to the United States. This framework generally allows for the transfer of EU data to U.S. entities that are certified with the U.S. Department of Commerce and comply with certain data privacy principles, set out by the EU Commission. However, the safe harbor concept only applies when transferring data to certain registered organizations and not to regulatory authorities. Thus, the safe harbor concept cannot be used in transferring data to U.S. regulators. Please also note that the validity of the Safe Harbor Framework has been put into question by Advocate General Bot, OPINION OF ADVOCATE GENERAL BOT delivered on 23 September 2015, Case C?362/14-Maximillian Schrems/ Data Protection Commissioner. In the Schrems case, an Austrian Facebook user challenged the U.S.-EU Safe Harbor Framework. In its opinion, the Advocate General stated that the EU Commission's Safe Harbor decision—which established the Safe Harbor Framework—is invalid because Europeans' personal data isn't adequately protected in the United States. Although the opinion is not binding, if the EU Court follows it, organizations may need to find an alternative legal basis for sending data from Europe to the United States.

8. In addition to the data privacy laws, there are various other restrictions to be aware of, including the banking secrecy and telecommunications laws, certain blocking statutes, and state secrecy laws.

Daily columns in the Law Journal report developments in laws affecting medical malpractice, immigration, equal employment opportunity, pensions, personal-injury claims, communications and many other areas.