Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

A GDPR Primer For U.S.-Based Cos. Handling EU Data: Part 2

By **Caroline Krass, Jason Kleinwaks, Ahmed Baladi and Emmanuelle Bartoli**
December 13, 2017, 1:18 PM EST

Caroline Krass

Jason Kleinwaks

Ahmed Baladi

Emmanuelle Bartoli

The General Data Protection Regulation (GDPR), a new European Union data privacy and protection regime, has already entered into force and is slated to become effective on May 25, 2018. Designed to provide greater protections to the personal data of individuals located in the EU, the GDPR imposes a host of new obligations on both "controllers" and "processors" of such data. Additionally, the GDPR calls for large penalties when companies fail to comply with these new obligations.

While many U.S. companies have already begun the process of bringing themselves into compliance, the GDPR has such a long reach that it may encompass a large subset of U.S. organizations that would not ordinarily expect to be subject to European data privacy laws. Smaller organizations or those that deal with a relatively small amount of data originating in the EU may be especially likely to be caught off-guard. The purpose of this article is to increase awareness of possible GDPR obligations among these organizations, as well as to explain the different EU-approved mechanisms for the transfer of data from the EU to the United States for processing. Such organizations must take immediate steps to assess whether they are subject to the new GDPR and to bring themselves into compliance.

In part one of this two-part series, we outlined the global scope of the GDPR, the organizations that may be required to comply with its requirements, and the obligations that the GDPR imposes on controllers and processors. In this second and final part of the series, we explain the stringent restrictions placed on cross-border data transfers to countries outside of the EU, various compliance mechanisms and penalties, and potential deviations in implementation among EU member states. Finally, we include some practical advice for organizations transitioning to the new regime.

———

How Can U.S. Organizations Comply with Restrictions on Transferring EU Personal Data to the U.S.?

The 1995 EU Data Protection Directive (1995 EU directive) significantly restricts the transfer of EU personal data to third countries, and these restrictions continue under the

GDPR. Both the 1995 EU directive and the GDPR allow for transfers of personal data out of the EU when the data are being sent to a country that the European Commission (EC) has determined provides an adequate level of protection.[1] But the United States is conspicuously absent from the list of countries that have received an EC adequacy decision. Transfers to countries which have not received the EC's blessing, like the United States, must either fall within one of the various derogations[2] in the directive (or regulation) or the parties involved in the transfer themselves must provide adequate assurances that the data will be protected. Because the GDPR requires the same protections be carried over for "onward transfers" or transfers following the initial third-country transfer, compliance with transfer requirements is important for any organization down the chain.

Adequate assurances of data protection can be made in a number of ways, including:

EU-U.S. Privacy Shield

Between 1998 and 2000, the International Safe Harbor Principles were developed in order to provide an alternate mechanism by which U.S. companies could comply with the 1995 EU directive's data transfer requirements. Safe Harbor provided a framework of seven data protection principles, and companies could self-certify under the program. In July of 2000, the EC determined that companies complying with the safe harbor principles could transfer EU personal data to the United States in compliance with the directive. But a combination of factors, including the rapid expansion of global online activities and their importance to the transatlantic economy; the rapid increase in the number of U.S. companies taking advantage of the safe harbor principles; and the controversy resulting from Edward Snowden's 2013 leaks of classified information related to U.S. government surveillance activities threw the continuing viability of Safe Harbor into question.[3] In 2015, the European Court of Justice struck down its previous decision that the safe harbor program provided adequate protections for data transferred to the United States.[4]

Consequently, the U.S. government began talks with the EU seeking to develop a new framework. In February of 2016, a political agreement was reached to implement the new Privacy Shield program. Despite concerns raised by the Article 29 Data Protection Working Party[5] (Article 29 working party or working party) and the EU data protection supervisor, the EC adopted the framework in July of 2016.

The 2016 EU-U.S. Privacy Shield allows participating organizations to transfer EU personal data to the United States. Organizations must self-certify as Privacy Shield-compliant, committing to process data only in accordance with the principles set forth by the program.[6] Only organizations subject to the enforcement authority of the Federal Trade Commission or the U.S. Department of Transportation are eligible to participate.

Despite the concerns raised by some groups, the Privacy Shield recently successfully passed its first annual review[7] by the EC, with the relatively lukewarm endorsement that the "Privacy Shield works well, but there is some room for improving its implementation."[8] While the EC found that the framework provides an adequate level of protection for personal data, it made five key recommendations to ensure continued protection[9]:

- More proactive and frequent monitoring by the U.S. Department of Commerce conduct to ensure that self-certified companies are complying with their Privacy Shield obligations, including regular searches to find companies making false claims about their participation in the Privacy Shield. During the first year of implementation, only three enforcement actions have

been reported.[10]

- Increased attention to making EU data subjects aware of how to exercise their rights under the Privacy Shield, including how to lodge complaints.

- Increased cooperation between the Department of Commerce, the Federal Trade Commission, and the EU Data Protection Authorities (DPAs), including in developing guidance for enforcers and companies alike.

- Federal legislation to make permanent the protection for non-Americans offered by Presidential Policy Directive 28 (PPD-28). PPD-28 is an Obama-era limitation on the collection of signals intelligence that requires appropriate safeguards for all personal information, regardless of whether they are U.S. or foreign.[11]

- The appointment of a permanent Privacy Shield ombudsman at the U.S. State Department to provide European citizens with a recourse mechanism and the filling of numerous vacancies on the Privacy and Civil Liberties Oversight Board (PCLOB).

The continued viability of the Privacy Shield may hinge on the Trump administration's response to these recommendations. The four vacant PCLOB positions require presidential appointment and Senate confirmation. President Donald Trump has explained in general that many vacancies across federal departments have not been filled because the administration believes the underlying positions are unnecessary. While it remains unclear whether and how quickly the ombudsman and PCLOB vacancies will be filled, the Trump administration recently nominated Adam Klein as the PCLOB's chairman. It also remains unclear whether the administration would support the codification of PPD-28's protections for non-U.S. persons.

Following the EC's review of the Privacy Shield, the Article 29 working party conducted its own review, which took a more critical view than that of the EC.[12] While the working party characterized the Privacy Shield as an improvement over the previous safe harbor framework, it echoed many of the concerns raised by the EC, including the need for the appointment of an ombudsman and members of the PCLOB. Unlike the EC, the working party warned that it would "take appropriate action, including bringing the Privacy Shield adequacy decision to national courts for them to make a reference to the [European Court of Justice] for a preliminary ruling" if action is not taken by the time of the next annual review.

In spite of these concerns, over 2,400 companies currently participate in the Privacy Shield. For U.S. companies that routinely receive transfers of EU personal data, the Privacy Shield provides the easiest method of ensuring compliance with the EU data regimes, present and future, and also affords those companies goodwill with their European customers.

Standard Contractual Clauses[13]

Another popular way to comply with the EU data regimes while transferring personal data to third countries that have not received an adequacy decision from the EC is through standard contractual clauses (SCCs) approved by the EC. Through the use of SCCs embedded in contracts between a data exporter and a data importer, the parties guarantee an adequate level of protection for the personal data involved in the transaction. The EC has adopted SCCs for controller-to-processor and controller-to-

controller transactions, which will, for now, continue to provide an adequate level of protection for personal data involved in transfers. Under the 1995 EU directive, only the EC was permitted to adopt SCCs, but the GDPR permits national supervisory authorities to adopt SCCs as well.[14] SCCs remain a burdensome approach to data transfers because, in practice, data protection authorities require organizations to enter into SCCs to cover each new purpose of processing.

The SCCs have been under legal attack on the theory that U.S. law fails to adequately provide legal remedies to EU citizens and that the SCCs do not address that deficiency. Recently, the Irish High Court in Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems[15] referred the issue to the EU Court of Justice to assess whether the EC's prior decisions approving the SCCs remain valid, finding that the Irish data protection controller's concerns regarding the continued validity of SCCs are "well-founded," primarily in light of concerns regarding remedies available in the United States to EU data subjects. Still, SCCs remain one of the most common legal methods utilized to effect personal data transfers out of the EU.

Binding Corporate Rules[16]

While the 1995 EU directive did not expressly recognize binding corporate rules (BCRs) (which were created by the Article 29 working party), the GDPR explicitly codifies the possibility for organizations to adopt BCRs. BCRs are legally binding internal rules that can be adopted by either multinational groups of undertakings, or groups of enterprises engaged in a joint economic activity (i.e., groups of legally independent entities). The GDPR introduces regulatory requirements related to BCR content and a simplified approval process. Compared to the SCCs and Privacy Shield framework, BCRs offer an opportunity for more customization that is tailored to the needs of the adopting group of companies. BCRs are also seen by data protection authorities as providing more legal certainty to data transfers. Moreover, BCRs are seen as a tool for accountability because the requirements companies must comply with when adopting BCRs will assist the companies' efforts in structuring their data protection governance.

Codes of Conduct and Certifications[17]

Companies can also demonstrate compliance with the GDPR through codes of conduct[18] and certification[19] mechanisms. Codes of conduct are prepared by associations or bodies representing categories of controllers or processors and must go through a specified approval process that differs depending on whether it governs processing activities in a single EU state or in several states.[20] Compliance will be monitored by an independent body with relevant expertise and accredited by the appropriate supervisory authority.[21] Certification mechanisms, seals or marks, on the other hand, might be established by the supervisory authorities, European Data Protection Board and the EC in the future as a way similarly to demonstrate compliance.[22] Adherence to a code of conduct or certification mechanism, if binding and enforceable, can be used to demonstrate appropriate safeguards for data transfers to third countries. The viability of these new mechanisms under the GDPR remains to be seen.

Compliance with U.S. Court Rulings or Subpoenas Requiring Production of EU Personal Data

Significantly, Article 48 of the GDPR could impede a company's ability to comply with the U.S. legal process requiring the production of EU personal data. Under this provision, any judgment of a court or decision by an administrative authority of a third country that would require transfer or disclosure of EU personal data is only recognizable and enforceable if based on an international agreement, such as a

mutual legal assistance treaty between the third country and the EU or a particular member state. Although the United States and the EU have entered into a binding mutual legal assistance agreement (MLAA),[23] Article 48 may present challenges where there is a conflict between U.S. legal process and the requirements of the MLAA. Further, if the U.S. courts' collective disregard for European blocking statues is any indication of how they will approach this provision of the GDPR, we may find that courts are particularly unsympathetic to the claim that production would violate the GDPR, potentially placing companies in the difficult position of choosing whether to comply with the U.S. legal process or the GDPR.

What Are the Compliance Mechanisms and Penalties for Noncompliance with the GDPR?

The GDPR grants investigative powers to the member states' supervisory authorities that are roughly consistent with those under the 1995 EU directive,[24] and controllers and processors are obligated to cooperate with supervisory authorities on request.[25] Supervising authorities are also given an array of corrective powers[26] with which to address infringements of the GDPR, including the ability to issue warnings or orders and impose administrative fines. Maximum fines for violations of specific articles are provided, topping out at the greater of either 20,000,000 euros or 4 percent of the total worldwide annual turnover from the preceding financial year.[27]

The GDPR also creates a right to compensation for any person who has suffered material or nonmaterial damage as a result of an infringement of the obligations in the regulation.[28] For the first time, a processor is directly liable for damage caused by processing that does not comply with GDPR obligations specifically directed to processors or where it has acted contrary to the controller's lawful instructions unless the processor can prove that it is not "in any way responsible for the event giving rise to the damage."[29] A data subject's claim under Article 82 of the GDPR is without prejudice to any claims involving the violation of other provisions of EU or member state law.[30]

Data subjects may lodge a complaint with a competent supervisory authority for violations of the GDPR.[31] They may also seek a judicial remedy against a controller or processor before the courts of the member state in which the controller or processor has an establishment or where the data subject habitually resides.[32] Additionally, both data subjects and controllers/processors can seek a judicial remedy against legally binding decisions of a supervisory authority in the courts of the member state in which the supervisory authority is established.[33]

Will EU Member States Uniformly Apply the GDPR?

While the GDPR was designed to provide a more uniform data regime across the EU than its predecessor directive, which required implementing legislation in each member state, it includes a number of opening clauses that allow member states to introduce particularized legislation in certain areas of data protection. Organizations should therefore pay close attention to any national distinctions that develop as member states begin to pass such legislation. In particular, the GDPR allows for member states to set general data protection requirements involving the processing of employee personal data that align with their respective labor law regimes.[34] Notably, most European countries are currently working on the adoption of national legislation that intends to embody the GDPR's requirements. The risk, however, is that each national legislature will introduce its own specific constraints.

In October 2017, the Article 29 working party issued guidance with the stated objective of helping supervisory authorities across the EU to apply administrative fines consistently.[35] Given the general nature of the criteria to apply, uniformity will be challenging to achieve.

Germany

The German Parliament recently adopted the new Federal Data Protection Act (the DPA),[36] which will come into force simultaneously with the GDPR on May 25, 2018, and which is meant to implement the GDPR into German law. During the legislative process, Germany made use of several opening clauses contained in the GDPR to maintain certain well-established provisions of the old DPA. However, the EC has questioned whether all new provisions in the DPA are actually covered by these opening clauses; in fact, some European officials noted off the record that the new DPA may undermine the goal of full harmonization within the EU.

Important deviations from the GDPR include:

- **Appointment of Data Protection Officers:** The DPA requires the appointment of a DPO by every company employing at least 10 persons that is involved in the automatic processing of personal data. Further, regardless of the number of employees, companies are obliged to appoint a DPA if they are processing data for the purpose of commercial transfer of data or for marketing and market research purposes.

- **Consumer Damage Claims:** Consumers are entitled to monetary compensation if they are affected by a violation of the DPA even if they did not suffer monetary damages. This may lead to increased risks for organizations as the new right for consumer protection associations to launch class-action-style proceedings facilitates the enforcement of corresponding claims.

The United Kingdom

Respecting the results of a national referendum that took place on June 23, 2016, the U.K. government gave the European Council formal notification of the U.K.'s intention to withdraw from the EU (Brexit) on March 29, 2017. Absent an extension agreed upon by all other member states, the U.K. will leave the EU at midnight on March 29, 2019.

In preparation for Brexit, the U.K. government is planning to enact national legislation that would continue to apply GDPR-compliant standards of data protection in the U.K. after Brexit. It is hoped that an agreement will be reached under which U.K. laws are acknowledged by the EU to provide an adequate level of protection post-Brexit, thus permitting data transfers between EU countries and the U.K. without the usual restrictions applying to "third-country" transfers (see the section titled "How Can U.S. Organizations Comply with Restrictions on Transferring EU Personal Data to the U.S.?" above). While transfers of data between the U.K. and U.S. may fall outside the EU-U.S. Privacy Shield after Brexit, it is hoped that a similar U.K.-U.S. agreement will maintain free data flows with the U.S. post-Brexit.

How Can Organizations Prepare for the GDPR?

As the implementation date for the GDPR approaches, organizations need to bring their operations into compliance with the new regime. The very first step an organization must take is to determine whether it is covered by the GDPR. If so, the organization must make efforts to fully understand what data it collects, processes, and stores. An organization must identify what personal data is being gathered across all of the organization's groups and functions and determine the purpose for collection, whether

that collection is being minimized to meet only that purpose, and whether the company is collecting any of the various types of sensitive data under the GDPR.

Beyond collection of data, the organization must understand how the data is being processed and stored. This includes the lawful basis for processing each set of data, data protection measures that are being used, the location of the stored data, the period of time such data will be stored, where and how records of processing and storage are being kept, and many other considerations. Obtaining all of this information will likely require a company-wide audit and stakeholders in all aspects of the business should be involved in this assessment. Often, collection and processing activities take place in departments that are not normally associated with data processing. Thus, data mapping is an important first step in determining what changes an organization must make to bring itself into compliance with the GDPR.

On top of the collection, processing and storage considerations, organizations must be aware of how they transfer and share data. As discussed above, the GDPR places restrictions on data transfers, especially those in which data is transferred across borders to countries outside the EU. These considerations apply regardless of whether such transfers take place only within the company or group of companies. Further, companies that transfer data to processors or sub-processors will need to reevaluate their contractual relationships with such processors, as well as the capabilities of the processor.

After data mapping and auditing, the company should put together a plan to bring itself into compliance with the GDPR. Processing activities that imply processing of sensitive personal data or that relate to purposes implying intrusion into data subjects' lives should be given top priority. The compliance plan should include specific training needs, as well as legal and technological elements that need to be addressed. Again, stakeholders in all aspects of the business should be involved in order to best implement organization-wide changes.

Data management will likely require significant thought and investment moving forward. Organizations must comply with GDPR requirements surrounding deletion of data, limitations on its use and ensuring adequate security measures are in place. Systems and processes must be in place to comply with requests from data subjects, such as providing copies of data, transferring data to other controllers, rectifying errors and even erasure in certain cases. Record-keeping may require further investment, as organizations will have to maintain detailed records of their processing and compliance with the GDPR. Data controllers should reconfigure their privacy policies to properly notify individuals of processing, making sure to comply with GDPR principles governing transparency and consent.

Organizations may even need to make changes to their corporate governance. As discussed above, some organizations will be required to obtain a DPO to monitor GDPR compliance, serve as a contact for regulators and oversee data impact assessments. The DPO can either exist within the organization or externally, but every indication is that the DPO must be highly knowledgeable both in terms of data privacy expertise and awareness of the inner workings of the organization. Because of requirements relating to the independence of the DPO, organizations should give significant thought to the organizational placement of the DPO and to whom the DPO should report within the corporate structure. Even where a DPO is not required, organizations should reevaluate their current privacy team to account for ongoing compliance requirements under the GDPR, such as data impact assessments, handling requests from data subjects, interfacing with regulators and ensuring adequate record-keeping. Many larger, data-driven businesses have approached regulators with their current plans to obtain their input.

Conclusion

When the GDPR takes effect in May of 2018, it will take some time to sort out some of the ambiguities that exist and to understand how enforcement is being carried out. Nonetheless, organizations should make concerted efforts to comply with the terms of the regulation from its outset, especially given the potential for such weighty penalties. Any concerns should be discussed with counsel well in advance of the GDPR's effective date in order to ensure a smooth transition to the new regime.

Caroline Krass is a partner in the Washington, D.C., office of Gibson Dunn & Crutcher LLP. Jason N. Kleinwaks is an associate attorney in the firm's Washington, D.C., office. Ahmed Baladi is a partner in the firm's Paris office. Emmanuelle Bartoli is an associate attorney in the firm's Paris office.

[1] Art. 45, GDPR.

[2] Art. 49, GDPR.

[3] See European Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, Section 1 (Dec. 7, 2016). http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.

[4] Maximillian Schrems v. Data Protection Commissioner, Case C-362/14 (Oct. 6, 2015). http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1444299455884&uri=CELEX:62014CJ0362.

[5] The Article 29 working party is the independent European Union Advisory Board on Data Protection and Privacy established under Article 29 of the 1995 EU directive.

[6] Privacy Shield Framework. https://www.privacyshield.gov/article?id=OVERVIEW.

[7] First Annual Review of the EU-U.S. Privacy Shield (Oct. 18, 2017). http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619.

[8] EU-U.S. Privacy Shield: First review shows it works well but implementation can be improved (Oct. 18, 2017). http://europa.eu/rapid/press-release_IP-17-3966_en.htm.

[9] Id.

[10] Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework, Federal Trade Commission (Sept. 8, 2017). https://www.ftc.gov/news-events/press-releases/2017/09/three-companies-agree-settle-ftc-charges-they-falsely-claimed.

[11] Sec. 4, Presidential Policy Directive 28 (Jan. 17, 2014). https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[12] EU – U.S. Privacy Shield – First Annual Joint Review, Article 29 Data Protection Working Party (Nov. 28, 2017). http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782.

[13] Art. 46, ¶ 2(c) GDPR.

[14] Art. 46, ¶ 2(d), GDPR.

[15] Irish Data Protection Commissioner v. Facebook and Max Schrems, 2016 No. 4809 P. https://arstechnica.co.uk/wp-content/uploads/sites/3/2016/07/Judgment-of-the-High-Court-of-Ireland-in-the-case-data-protection-Commissioner-v-Facebook-relating-to-motions-to-allow-amicus-curia.pdf

[16] Arts. 46, ¶ 2(b) & 47, GDPR.

[17] Art. 46, ¶¶ 2(e) & (f), GDPR.

[18] Arts. 40 & 41, GDPR.

[19] Arts. 42 & 43, GDPR.

[20] Art. 40, GDPR.

[21] Art. 41, GDPR.

[22] Arts. 42 & 43, GDPR.

[23] Agreement Between the United States of America and the European Union (signed June 25, 2003; entered into force Feb. 1, 2010). https://www.state.gov/documents/organization/180815.pdf.

[24] Art. 58, ¶ 1, GDPR.

[25] Art. 31, GDPR.

[26] Art. 58, GDPR.

[27] Art. 83, ¶¶ 4–5, GDPR.

[28] Art. 82, ¶ 1, GDPR.

[29] Art. 82, ¶¶ 2–3, GDPR.

[30] Rec. 146, GDPR.

[31] Art. 77, ¶ 1, GDPR.

[32] Art. 79, GDPR.

[33] Art. 78, GDPR.

[34] See Art. 88, ¶ 1, GDPR.

[35] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, Article 29 Data Protection Working Party (Oct. 3, 2017). https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889.

[36] Federal Data Protection Act (June 30, 2017). https://iapp.org/media/pdf/resource_center/Eng-trans-Germany-DPL.pdf.