GIBSON DUNN

December 4, 2017

THE GENERAL DATA PROTECTION REGULATION: A PRIMER FOR U.S.-BASED ORGANIZATIONS THAT HANDLE EU PERSONAL DATA

To Our Clients and Friends:

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. Such organizations must take immediate steps to assess whether they are subject to the new GDPR and to bring themselves into compliance.

This client alert lays out the global scope of the GDPR and describes which organizations may be required to comply. Next, we explain the obligations that the GDPR imposes on controllers and processors, as well as the stringent restrictions placed on cross-border data transfers to countries outside of the EU. We then provide an overview of the various compliance mechanisms and penalties the GDPR includes, and potential deviations in the implementation of the GDPR that might be seen in particular EU member states. Finally, we conclude with practical advice for organizations transitioning to the new regime.

As 2017 draws to an end, U.S. companies that handle the personal data of individuals located in the European Union (EU) are closer to confronting a new data security and privacy regime that will require an increased focus on compliance, even where such companies do not have establishments in the EU. Though it has already entered into force, the EU's General Data Protection Regulation[1] (GDPR) will take effect on May 25, 2018, formally replacing the 1995 EU Data Protection Directive[2] (1995 EU Directive) as the framework governing the processing of personal data across EU Member States. The GDPR is intended to provide greater protections to personal data belonging to individuals located in the EU, as well as greater consistency in application across the Union. Significantly, the GDPR will impose new obligations on organizations involved in the processing of EU personal data. Fines under the GDPR will likely vary significantly, with a maximum of the greater of either €20,000,000 or 4% of annual worldwide turnover, depending on the seriousness of the violation.

While large, data-driven companies with a global footprint are likely already well-aware of the GDPR, U.S. organizations that handle even small amounts of EU personal data may be surprised to find themselves subject to the GDPR and need to take steps to bring themselves into compliance before the regulation goes into effect. One significant change is that while the 1995 EU Directive currently places the burden of compliance on controllers of personal data, the GDPR creates direct obligations and liability for processors, including those based in the U.S. In other words, the GDPR rebalances obligations between companies requesting services (controllers) and companies offering services (processors). The purpose of this client alert is to increase awareness of possible GDPR obligations among smaller U.S. organizations, organizations in which data processing is not a large proportion of their business, and organizations that do not have a large European footprint but may nonetheless handle some data belonging to persons located in the EU, as well as to explain the different EU-approved mechanisms for the transfer of data from the EU to the United States for processing. Because controllers and processors may incur both large penalties and liability for non-compliance with the GDPR, and because it will take time to bring programs into compliance, the time is now for entities involved in the processing of EU personal data to familiarize themselves with the relevant requirements of the GDPR and to work on implementation of any necessary changes.

1. Who Must Comply with the GDPR?

First and foremost, U.S. organizations that interact with the EU market and/or that have entities in the EU should assess whether they will be required to abide by the GDPR when it takes effect in May 2018. The GDPR applies to organizations involved in the processing of personal data of individuals located in the EU. "[P]ersonal data" is defined broadly as "any information relating to an identified or identifiable natural person."[3] "Processing" means "any operation or set of operations which is performed on personal data or on sets of personal data."[4] These are broad definitions encompassing a range of data types and a variety of data usages—they are designed in particular to sweep in U.S. technology companies. Indeed, information such as log-in information, IP addresses, and vehicle identification numbers, though not enabling direct identification of individuals, allow for identification of individuals indirectly and are therefore considered to be personal data. This means that, in practice, most services and/or projects will be considered to involve processing of personal data. Also important to note is the possibility that, because these definitions—particularly the definition of personal data—are specific to the EU and the GDPR, U.S. companies may be less familiar with their scope and contours.

Organizations involved in processing personal data are divided into two categories: "controllers" and "processors." A controller, acting alone or together with others, "determines the purposes and means of the processing of personal data."[5] A processor, on the other hand, "processes personal data on behalf of the controller."[6] These definitions remain essentially unchanged from the 1995 EU Directive, and thus an entity that qualifies as a controller or processor under the 1995 EU Directive will likely continue to be a controller or processor under the GDPR.

However, the GDPR significantly expands the territorial reach of EU data laws, applying its requirements to three specific categories of entities:

- First, a controller or processor that maintains an "establishment" in the EU will be subject to the GDPR if it processes personal data "in the context of" that EU establishment, *regardless of whether the processing actually takes place in the EU*.[7] While the term "establishment" is not defined, the GDPR explains that "effective and real exercise of activity through stable arrangements" will satisfy the provision.[8] Additionally, "[t]he legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect."[9] In other words, the regulation may apply even if an organization's nexus to the EU is less formal than a parent-subsidiary relationship.

- Second, a controller or processor not established in the EU will be subject to the GDPR "where the processing activities are related to offering goods or services to data subjects in the Union," even when the goods and services are offered for free.[10] Determining whether an entity "envisages" offering goods or services in at least one EU Member State, thereby triggering the GDPR's requirements, depends on "factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union."[11]

- Third, a controller or processor not established in the EU will be subject to the GDPR if it processes the personal data of data subjects in the EU and that processing is related to the "monitoring" in the EU of the "behavior" of data subjects as their behavior takes place within the EU.[12] Processing fits within this definition when "natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."[13] This internet profiling is just one example of what monitoring can entail. Physical monitoring may also be included, such as by video camera recording.

Organizations, including U.S.-based companies, that fall within any of these three categories will be required to comply with the numerous obligations imposed by the GDPR.

2. What Obligations Does the GDPR Create for Controllers?

The GDPR imposes many obligations on controllers of EU personal data. Some of these obligations are a continuation of those established by the 1995 EU Directive, but others are either new or expanded. These obligations can be organized into three different streams: (i) principles applicable to the processing of personal data; (ii) data subjects' rights, and (iii) accountability.

2.1 Principles Applicable to the Processing of Personal Data

- Lawful Basis for Processing:[14] Processing of EU personal data may only be undertaken if the controller has a lawful basis for that processing under the GDPR. Permissible lawful bases are listed in Article 6 of the GDPR and include: (1) processing necessary for the performance of or entry into a contract with a particular data subject; (2) processing necessary for compliance with a legal obligation to which the controller is subject under EU or Member State law; (3) processing necessary to protect the "vital interests" of the data subject or of another natural person;

(4) processing necessary for the performance of a task in the public interest or in the exercise of official authority vested in the controller; or (5) processing necessary for the purposes of legitimate interests pursued by the controller or third party, "except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject."

Where the controller cannot rely on any of the five legal bases set forth above, it will need to obtain the individual's express consent. To be valid, consent must be freely given, specific, informed and unambiguous. Controllers intending to rely on consent will therefore need to make sure that they implement a mechanism that actually enables them to collect and monitor where consent is actually obtained (e.g., a clear banner or a box to be ticked specifically consenting to the purposes for processing). When personal data are to be processed for a purpose other than the one for which the data have been collected initially, the controller must consider whether the new purpose is compatible with the original purpose of processing, and if not, the controller will need to ensure that it relies on one of the five legal bases described above.[15]

- Delegation to a Processor: When a controller enlists a processor to process personal data on its behalf, the controller must use only processors that provide, by a binding written contract or other legal act, sufficient guarantees that they will implement appropriate safeguards required by the GDPR and ensure the protection of EU data subjects' rights.[16] Any sub-processor must also commit in a binding written contract (or other legal act) to abiding by the same safeguards.[17] The contract must specify the subject matter and duration of the processing; the nature and purpose of the processing; the type of personal data; the categories of data subjects; and the obligations and rights of the controller.[18] Thus, controllers should reevaluate their contractual relationships with processors in advance of the effective date of the GDPR. Agreeing to EC-approved standard contractual clauses, discussed further below, is one option for seamlessly complying with such requirements.

- Specific Contractual Obligations:[19] In addition to requiring a contractual relationship between controllers and processors, the GDPR mandates a host of stipulations that must be included in such contracts: (1) processing must be performed only in accordance with documented instructions from the controller; (2) persons authorized to process personal data must have committed themselves to confidentiality or be subject to a statutory obligation of confidentiality; (3) processors must implement requisite security measures; (4) processors must abide by the requirements for enlisting sub-processors; (5) processors must assist the controller in fulfilling the controller's obligation to respond to requests for exercising data subjects' rights under the GDPR; (6) processors must assist the controller in complying with requirements for data security and breaches; (7) personal data must be deleted or returned to the controller after processing services have been rendered; (8) all information necessary to demonstrate compliance with these requirements must be made available to the controller, and (9) the processor must allow for and contribute to audits conducted by the controller.

- Data Breach Notification:[20] In the event of a data breach, the controller must notify the supervisory authority "without undue delay" and within 72 hours of discovering the breach, where feasible. Any delay must be explained. In practice, this 72-hour deadline may be difficult

to meet given the nature of detecting data breaches and determining their extent. Additionally, if the data breach is likely to result in a "high risk to the rights and freedoms of natural persons," the controller must notify the affected data subjects without undue delay, unless one of a number of exceptions is triggered.[21]

2.2 Individuals' Rights

- Information and Access: Controllers must provide certain specified information to data subjects at the time personal data is obtained.[22] This information is designed to ensure fair and transparent processing, and it is particularly important where the controller will intend to rely on consent. Minimum information required by the GDPR includes the purpose of processing; the categories of data recipients; the existence of data transfers out of the EU and the guarantees implemented in case of such transfer; the data retention period; and data subjects' rights. Data subjects also have a right to request and obtain specified information from the controller about the processing of their personal data as well as a copy of the personal data undergoing processing.[23]

- Rectification and Erasure: Controllers are obligated to allow data subjects to correct inaccurate personal data and add to incomplete personal data.[24] Further, controllers must accommodate data subjects' requests to have their personal data erased without undue delay if certain grounds apply, including if the personal data is no longer necessary for the purposes it was originally collected or processed.[25]

- Data Portability:[26] Upon request from a data subject, controllers must provide a data subject's personal data in a machine-readable format or transmit that personal data directly to another controller.

2.3 Accountability

Organizations are expected to be accountable in relation to the processing of personal data. Consequently, they will need to implement several governance measures to demonstrate and document their compliance.

- Record-Keeping:[27] The GDPR represents a change of paradigm for companies. Under the 1995 EU Directive currently in force, companies are expected to give notice to competent data protection authorities prior to engaging in certain processing activities. The GDPR removes prior notice obligations and instead requires controllers to maintain records of all processing activities, including certain specified types of information. The purpose of these records is to allow the controller to demonstrate compliance with GDPR requirements, and records must be made available to the relevant supervisory authority upon request. To comply with this obligation, organizations must begin conducting data protection audits to make an inventory of the different personal data processing activities carried out within the organization. Organizations that do not begin to implement record-keeping as the effective date of the GDPR approaches will certainly face difficulties in complying with the GDPR's requirements. (Note that these requirements do

not apply to a controller employing fewer than 250 people unless it carries out high-risk processing, carries out more than occasional processing, or processes special categories of data.)

- Data Protection Officer: As part of the cultural change in data protection management, the appointment of a Data Protection Officer (DPO) is also specified by the GDPR.[28] Indeed, controllers may be required to appoint a DPO when: (i) the core activities of the controller are processing operations that require large-scale, regular and systematic monitoring of data subjects or, similarly, (ii) when a controller's core activities involve large-scale processing of other special categories of data.[29] DPOs are responsible for accountability of the controller, must be included in all matters relating to the protection of personal data, and "act as intermediaries between relevant stakeholders."[30] In doing so, DPOs must be given a sufficient degree of autonomy to perform their required tasks under GDPR Article 39.[31] DPOs are assured independence and job security through the GDPR's prohibition on dismissing or penalizing a DPO "for performing [their] tasks."[32] In practice, organizations need to consider whether they are subject to the obligation of appointing a DPO. Even where not strictly necessary, companies may still consider whether having a DPO would help in complying with the different obligations defined by the GDPR.

- Data Protection Impact Assessment:[33] Where the controller undertakes a type of processing that is likely to result in a high risk to the rights and freedoms of natural persons, the controller must carry out an impact assessment of that processing, in consultation with any designated DPO. While the supervisory authority is required to create a list of processing operations that require an impact assessment, the GDPR specifies several scenarios in which impact assessments are required. It also provides requirements for the content of such assessments. Where an impact assessment indicates that processing would "result in a high risk in the absence of measures taken by the controller to mitigate the risk," the controller must consult with the supervisory authority prior to undertaking the processing.[34] This obligation indicates that companies will need to have a risk-based approach in relation to data protection.

- "Data Protection by Design and by Default":[35] All controllers must implement appropriate technical and organizational safeguards to ensure that any processing of personal data complies with the GDPR, including, as appropriate, data protection policies, data minimization, and "pseudonymisation."[36] Controllers should take into account both the cost of such safeguards, as well as the protections current technology allows, adapting to the risks posed by the processing to the "rights and freedoms" of EU data subjects.[37] Adherence to approved codes of conduct or certification mechanisms, discussed further below, is one way to demonstrate compliance.

- Designated Representatives:[38] When a controller is not established in the EU but is nonetheless subject to the GDPR, the controller in certain circumstances must designate a representative in a Member State where the EU individuals whose personal data is being processed in connection to the offering of goods and services, or whose behavior is being monitored, are located. This requirement does not apply when the processing is occasional or when the processing does not involve widespread processing of certain special categories of data, such as genetic and biometric data.

3. What Obligations Does the GDPR Create for Processors?

The GDPR creates a number of direct obligations for processors who fall within the scope of the regulation. While processors may have undertaken certain similar obligations by virtue of contracts with controllers in the past, the 1995 EU Directive does not itself impose such requirements on processors. While processors should carefully assess their new obligations with their legal counsel, the GDPR addresses the following topics:

- Data Security:[39] A processor is required to implement appropriate technical and organizational measures to ensure adequate data security. Assessment of the requisite security must take into account "the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed."

- Data Breach Notification:[40] In the event of a data breach, the processor must notify the controller "without undue delay."

- Following Controller's Instructions:[41] A processor may not process any personal data except in accordance with instructions from the controller. If a processor acts outside the scope of its authority granted by the controller, it will be considered to be a controller and subject to controller obligations under the GDPR.

- Contractual Relationships:[42] All processing by a processor on the controller's behalf must be governed by a binding contract "or other legal act" under EU or Member State law that specifically sets forth "the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects[,] and the obligations and rights of the controller." The contract must be in both written and electronic form.[43]

- Sub-Processing:[44] A processor may not utilize another processor in connection with its processing of EU personal data without first receiving authorization from the controller. The controller must be notified of any changes in sub-processers and given the opportunity to object. Where a sub-processor is engaged, the same data protection obligations in the contract between the controller and processor must be imposed on the sub-processor by way of contract or other "organisational measures."[45] The processor will remain fully liable to the controller for performance of the sub-processor's obligations.

- Designated Representatives:[46] As with controllers, see above, when a processor is not established in the EU but is still subject to the GDPR, it must designate a representative in one of the Member States in which one of the relevant data subjects is located, unless the processing is occasional or does not involve widespread processing of certain special categories of data.

- Record-Keeping:[47] Processors with 250 or more employees are required to maintain a record of all categories of processing activity carried out on behalf of a controller containing specific information. A processor with fewer than 250 employees need keep such records only if it is undertaking processing that is likely to result in a risk to the rights and freedoms of data subjects,

the processing is more than occasional, or the processing includes certain special categories of data relating to racial or ethnic origin, religious and other beliefs, sexual orientation, or criminal convictions and offenses. Records must be kept in written and electronic form, and must be made available to a supervisory authority upon request.

- Data Protection Officer:[48] In much the same way that controllers may be required to appoint a data protection officer, processors may also face such a requirement.

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

The 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.[49] 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[50] 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:

4.1 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.[51] 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.[52]

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 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.[53] Only organizations subject to the enforcement authority of the Federal Trade Commission or the Department of Transportation are eligible to participate.

Despite the concerns raised by some groups, the Privacy Shield recently successfully passed its first annual review[54] by the EC, with the relatively lukewarm endorsement that the "Privacy Shield works well, but there is some room for improving its implementation."[55] 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:[56]

- More proactive and frequent monitoring by the 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.[57]

- 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.[58]

- 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 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.

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.

4.2 Standard Contractual Clauses[59]

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.[60] 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*[61] 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.

4.3 Binding Corporate Rules[62]

While the 1995 EU Directive did not expressly recognize binding corporate rules (BCRs) (which were created by the Article 29 Working Party[63]), the GDPR explicitly codifies the possibility for organizations to adopt BCRs. BCRs are legally binding internal rules that can be adopted by either multi-national 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.

4.4 Codes of Conduct and Certifications[64]

Companies can also demonstrate compliance with the GDPR through Codes of Conduct[65] and Certification[66] 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.[67] Compliance will be monitored by an independent body with relevant expertise and accredited by the appropriate supervisory authority.[68] 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.[69] 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.

4.5 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),[70] 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.

5. What Are the Compliance Mechanisms and Penalties for Non-Compliance 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,[71] and controllers and processors are obligated to cooperate with supervisory authorities on request.[72] Supervising authorities are also given an array of corrective powers[73] 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 or 4% of the total worldwide annual turnover from the preceding financial year.[74]

The GDPR also creates a right to compensation for any person who has suffered material or non-material damage as a result of an infringement of the obligations in the regulation.[75] 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."[76] A data subject's claim under Art. 82 of the GDPR is without prejudice to any claims involving the violation of other provisions of EU or Member State law.[77]

Data subjects may lodge a complaint with a competent supervisory authority for violations of the GDPR.[78] 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.[79] 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.[80]

6. 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.[81] 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.[82] Given the general nature of the criteria to apply, uniformity will be challenging to achieve.

6.1 Germany

The German Parliament recently adopted the new Federal Data Protection Act (the "DPA"),[83] 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 ten 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.

6.2 The United Kingdom

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

In preparation for Brexit, the UK government is planning to enact national legislation that would continue to apply GDPR-compliant standards of data protection in the UK after Brexit. It is hoped that an agreement will be reached under which UK laws are acknowledged by the EU to provide an adequate level of protection post-Brexit, thus permitting data transfers between EU countries and the UK without the usual restrictions applying to "third country" transfers (see section 4 above). While transfers of data between the UK and U.S. may fall outside the EU-U.S. Privacy Shield after Brexit, it is hoped that a similar UK-U.S. agreement will maintain free data flows with the U.S. post-Brexit.

7. 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.

8. 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.

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[3] Art. 4, ¶ 1, GDPR.

[4] Art. 4, ¶ 2, GDPR.

[5] Art. 4, ¶ 7, GDPR.

[6] Art. 4, ¶ 8, GDPR.

[7] Art. 3, ¶ 1, GDPR.

[8] Rec. 22, GDPR.

[9] *Id.*

[10] Rec. 23, GDPR; *see also* Art. 3, ¶ 2(a), GDPR.

[11] Rec. 23, GDPR.

[12] Rec. 24, GDPR; *see also* Art. 4, ¶ 2(b), GDPR.

[13] Rec. 24, GDPR.

[14] Art. 6, ¶ 1, GDPR.

[15] Art. 6, ¶ 4, GDPR.

[16] Art. 28, ¶ 1, GDPR.

[17] Art. 28, ¶ 2, GDPR.

[18] Art. 28, ¶ 3, GDPR.

[19] Art. 28, ¶ 3 (a)–(h), GDPR.

[20] Art. 33, ¶ 1, GDPR.

[21] Art. 34, GDPR.

[22] Arts. 13 & 14, GDPR.

[23] Art. 15, GDPR.

[24] Art. 16, GDPR.

[25] Art. 17, GDPR.

[26] Art. 20, GDPR.

[27] Art. 30, GDPR

[28] Art. 37, GDPR.

[29] *Id.*

[30] *Guidelines on Data Protection Officers ('DPOs')*, Article 29 Working Party, at 4 (Dec. 13, 2016). http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

[31] *Id.* at 14.

[32] *Id.* at 15.

[33] Art. 35, GDPR.

[34] Art. 36, GDPR.

[35] Arts. 24 & 25, GDPR.

[36] *See also* Art. 32, GDPR.

[37] Art. 25, GDPR.

[38] Art. 27, GDPR.

[39] Art. 32, GDPR.

[40] Art. 33, ¶ 2, GDPR.

[41] Art. 29, GDPR.

[42] Art. 28, ¶ 3, GDPR.

[43] Art. 28, ¶ 9, GDPR.

[44] Art. 28, ¶ 2, GDPR.

[45] Art. 28, ¶ 4, GDPR.

[46] Art. 27, GDPR.

[47] Art. 30, ¶¶ 2–5, GDPR.

[48] Art. 37, GDPR.

[49] Art. 45, GDPR.

[50] Art. 49, GDPR.

[51] *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.

[52] *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.

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

[54] 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.

[55] 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.

[56] *Id.*

[57] *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.

[58] 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.

[59] Art. 46, ¶ 2(c) GDPR.

[60] Art. 46, ¶ 2(d), GDPR.

[61] *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

[62] Arts. 46, ¶ 2(b) & 47, GDPR.

[63] 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.

[64] Art. 46, ¶¶ 2(e) & (f), GDPR.

[65] Arts. 40 & 41, GDPR.

[66] Arts. 42 & 43, GDPR.

[67] Art. 40, GDPR.

[68] Art. 41, GDPR.

[69] Arts. 42 & 43, GDPR.

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

[71] Art. 58, ¶ 1, GDPR.

[72] Art. 31, GDPR.

[73] Art. 58, GDPR.

[74] Art. 83, ¶¶ 4–5, GDPR.

[75] Art. 82, ¶ 1, GDPR.

[76] Art. 82, ¶¶ 2–3, GDPR.

[77] Rec. 146, GDPR.

[78] Art. 77, ¶ 1, GDPR.

[79] Art. 79, GDPR.

[80] Art. 78, GDPR.

[81] *See* Art. 88, ¶ 1, GDPR.

[82] *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.

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

Gibson, Dunn & Crutcher's lawyers are available to assist in addressing any questions you may have regarding the issues discussed above. Please contact the Gibson Dunn lawyer with whom you usually work, any member of the firm's Privacy, Cybersecurity and Consumer Protection or National Security practice group, or the following authors:

Caroline Krass - Chair, National Security Practice, Washington, D.C. (+1 202-887-3784, ckrass@gibsondunn.com)
Alexander H. Southwell - Chair, Privacy, Cybersecurity & Consumer Protection Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Ahmed Baladi - Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
Emanuelle Bartoli - Paris (+33 (0)1 56 43 13 57, ebartoli@gibsondunn.com)
James A. Cox - London (+44 (0)20 7071 4250, jacox@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Jason N. Kleinwaks - Washington, D.C. (+1 202-887-3793, jkleinwaks@gibsondunn.com)