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 1

By **Caroline Krass, Jason Kleinwaks, Ahmed Baladi and Emmanuelle Bartoli**
December 12, 2017, 12:16 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. 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 lay out the global scope of the GDPR and describe which organizations may be required to comply. We also explain the obligations that the GDPR imposes on controllers and processors.

———

As 2017 draws to an end, U.S. companies that handle the personal data of individuals located in the 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 GDPR[1] 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 euros or 4 percent 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 article 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 noncompliance 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.

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 login 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.

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: (1) principles applicable to the processing of personal data; (2) data subjects' rights; and (3) accountability.

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 European Commission-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]

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.

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: (1) the core activities of the controller are processing operations that require large-scale, regular and systematic monitoring of data subjects or, similarly; (2) 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.

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.

Given the broad array of obligations imposed by the GDPR, organizations that handle the personal data of individuals located in the EU must begin to bring themselves into compliance as soon as possible. All organizations, including those that do not obviously operate in the EU, should assess the relevant requirements to determine whether they need to adhere to the regulation.

In the second part of this two-part series, we will 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. We will also offer some practical advice aimed at organizations that may have newfound obligations under the GDPR.

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] 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.