April 26, 2018

Implications of the New EU Data Protection Regime and Its Expanded Application for Non-EU Entities

The EU General Data Protection Regulation (the "GDPR"),[1] approved and adopted by the European Union in April 2016, takes effect in all member states of the European Union[2] on May 25, 2018. The GDPR replaces the 1995 EU Data Protection Directive[3] and is designed to provide greater protection to personal data of identified or identifiable natural persons in the European Union by imposing extended obligations on entities involved in the processing of such data. The GDPR is notable in that it significantly expands the territorial applicability of the EU data privacy laws (which now will also apply to non-EU entities that have established "controllers" or "processors" in the European Union or that are engaged in the processing of personal data of natural persons in the European Union regardless of whether such entities have established a presence in the European Union). The GDPR also strengthens the conditions for consent to personal data processing, creates direct obligations and liability for processors of personal data and imposes significantly increased penalties for non-compliance.

We summarize below the key provisions and obligations under the revised EU data protection regime, highlighting its potential implications for non-EU entities, and in particular those that do not have a presence in the European Union but that interact with natural persons who are in the European Union.

GDPR Scope and Applicability

The GDPR applies to a controller or processor (defined below) involved in the processing of personal data of identified or identifiable natural persons (referred to in the GDPR as "data subjects"). More

---

1 Regulation (EU) 2016/679, available here.

2 Since the GDPR is an EU regulation, rather than a directive, it will be directly applicable without the need for national implementing legislation in EU member states. In addition, the EFTA states of the EEA, *i.e.*, Iceland, Lichtenstein and Norway, are obligated to adopt the GDPR domestically as per Article 7(a) of the EEA Agreement. The draft of the EEA Joint Committee Decision on the incorporation of the GDPR into the EEA Agreement is currently under consideration by the European Union and the EEA EFTA states with the aim of being incorporated on June 1. More detail on the status of the GDPR incorporation into the EEA is available here. Once the GDPR is adopted into the domestic law of the EEA EFTA states, references in this Client Memorandum to EU member states can be instead read to apply to EEA EFTA member states as well unless the context requires otherwise.

3 Directive 95/46/EC, available here.

specifically, the GDPR expands the reach of the EU personal data protection laws to cover the following categories of controllers and processors:

- those that maintain an establishment in the European Union and process personal data "in the context of the activities of [such] establishment, regardless of whether the processing actually takes place in the [European] Union or not";
- those that are not established in the European Union and process personal data of "data subjects who are in the [European] Union" if their "processing activities are related to the offering of goods or services (. . .) to such subjects in the [European] Union," even if it is done for free; and
- those that are not established in the European Union and process personal data of "data subjects who are in the [European] Union" if the processing activities are related to monitoring of the behavior of such data subjects "as far as their behaviour takes place in the [European] Union."

The GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity that has no connection to a professional or commercial activity (such as correspondence and the holding of addresses or social networking), or by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences.

"Establishment"

The GDPR does not explicitly define the term "establishment" but explains that it would imply "effective and real exercise of activity through stable arrangements," although the legal form of such arrangement (*e.g.*, whether it is a branch or a subsidiary) would not be a determinative factor. A registered business in the European Union would fall within the definition, but ultimately the determination as to whether an entity has an establishment in the European Union must be based on the individual facts, looking at the nexus of the entity with the European Union. The Court of Justice of the European Union (the "CJEU") has, to date, interpreted the term "establishment," in the context of the prior EU data protection regime, very broadly. For example, in the *Google Spain* (2014) case, the CJEU held that EU data privacy law applied to processing conducted outside the European Union by a foreign data controller (the U.S. parent company, Google Inc.) that had an establishment in the European Union (through a subsidiary, Google Spain). The CJEU held that it was not necessary for the processing at issue to be carried out by the establishment itself (in this case, Google Spain) as long as it was carried out "in the context of its activities." It was ultimately held that "the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed."

"Processing"

Processing is defined as "any operation or set of operations which is performed on personal data or on sets of personal data." This is a broad definition that encompasses a range of data usages, such as the collection, recording, organization, structuring, storage, adaptation, disclosure by transmission and use or deletion of any information relating to a data subject.

"Offering of goods or services"

In order to determine whether a controller or processor is "offering goods or services to data subjects who are in the [European Union]," one should ascertain whether the controller or processor has intention or envisages offering services to data subjects in one or more EU member states. As provided in the recitals to the GDPR, "the mere accessibility of the controller's, processor's or an intermediary's website in the [European Union], of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established," will most likely be insufficient to show such intention. However, if the controller or processor of personal data uses the language or currency of an EU member state and facilitates ordering of goods or services in that other language or currency and allows shipping to local addresses or mentions customers who are in the European Union, it may "make it apparent that the controller envisages offering goods or services to data subjects in the [European Union]."

"Monitoring of behaviour"

In order to determine whether a processing activity involves monitoring of behavior of data subjects, one should ascertain whether data subjects "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."

In practice, the use of cookies and applications or IP addresses by controllers and processors to track the activity of their website users who are in the European Union could potentially be classified as monitoring of behavior of EU data subjects. On the other hand, a controller or processor not established in the European Union would most likely not be viewed as engaging in monitoring of behavior of EU data subjects if it simply maintains a website, which may be visited by EU data subjects, without the controller or processor taking further steps to process the information obtained on such data subjects through the website.

"Personal data"

Personal data is defined as data relating to a data subject who can be identified or is identifiable from the data. The GDPR definition of personal data encompasses a wider range of data types as it covers not only the traditional personal data, such as names, addresses, dates of birth or telephone numbers, but also includes the use of on-line identifiers, such as login information, IP addresses and cookies. Additionally, as noted in the recitals to the GDPR, any data that has undergone pseudonymisation but could be attributed to a natural person by the use of additional information should be considered personal data. On the other hand, the GDPR does not apply to processing of any anonymous information (*i.e.*, information that does not relate to an identified or identifiable natural person), including for statistical or research purposes.

Basic principles of the GDPR

Article 5 of the GDPR lists the key principles relating to the processing of personal data of data subjects:

- *lawfulness, fairness and transparency principle* – personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject;
- *purpose limitation principle* – personal data should be collected for a specified, explicit and legitimate purpose and processed only in a manner that is compatible with such purpose;
- *minimalization principle* – personal data collected and processed should be limited only to what is necessary in relation to the purposes for which the data are processed;
- *accuracy principle* – personal data that are processed must be accurate and, where necessary, kept up-to-date, and to the extent that the data are inaccurate they should be erased or updated without delay;
- *storage limitation principle* – personal data must be kept in a form that permits identification of the data subject for no longer than is necessary for the purposes for which the data are processed;
- *integrity and confidentiality principle* – personal data must be processed in a way that ensures appropriate security of such data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage; and
- *accountability* – controllers of personal data are responsible for demonstrating compliance with the above principles.

The application of these basic principles in the GDPR is more fully discussed below.

Processors and controllers and their obligations

The GDPR divides legal and natural persons (including public authorities, agencies and other bodies) that process personal data into two categories: (i) controllers that determine "the purposes and means of the processing of personal data" and (ii) processors that "process personal data on behalf of controllers."

The GDPR significantly expands the obligations of controllers and processors and, most notably, imposes direct compliance responsibility not just on controllers but also on processors of personal data. This could be of importance to non-EU entities (in particular, technology companies) that may have taken on a role of data processor since in the past such entities were not directly responsible for compliance with EU data privacy laws. Under the revised regime, such entities have expanded obligations and are directly responsible for compliance with the GDPR if they process personal data of individuals who are in the European Union, irrespective of where such processing occurs, how small or large they are or how significant the processing is to their business overall.

Controllers' obligations

The following is a summary of the obligations imposed on controllers of personal data under the GDPR.

- *Legal basis for processing* – a controller can only process personal data of data subjects if such processing has a legitimate basis. The GDPR provides the following six legal bases for personal data processing:
    - *Consent*: the data subject has given consent to the processing of his or her personal data for one or more specific purposes. The data subject's consent must be express, freely given, specific, informed and unambiguous. Accordingly, if a person gives consent without knowing the processing purpose in full and in an easy to understand way, then it will not be a valid consent. Silence, pre-ticked boxes or inactivity also do not constitute effective consent;
    - *Contract*: processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. A person cannot enter into a contract without providing some personal data and identifiers so that each contract by definition means that personal data are processed. Controllers, however, need to be careful so that the definition of contract is not used too broadly;
    - *Legal obligation*: processing is necessary for compliance with a legal obligation to which the controller is subject; however, controllers need to make sure that such processing has a basis in EU or a member state's law;

- *Vital interests*: processing is necessary in order to protect the vital interests of the data subject or another natural person. Vital interests are not defined in the GDPR;
- *Public interest*: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The GDPR leaves it to EU or an individual member state's law to determine whether the controller is performing a task in the public interest, which could include public health, social protection and scientific research; or
- *Legitimate interests*: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests of fundamental rights or freedoms of the data subject, in particular if a data subject is a child.

- *Delegation to processors* – in cases where a controller uses a processor to process personal data on its behalf, the controller may only use a processor of personal data that provides a binding written contract to abide by the GDPR's prescribed safeguards to ensure the safety of EU data subjects' personal data.
- *Specific contractual obligations for contracts with processors* – for contracts entered into between controllers and processors of personal data, the GDPR prescribes a number of mandatory provisions, such as the requirement for document instructions, confidentiality undertakings, implementation of specified security measures and others.
- *Security of data processing* – the controller is required to implement appropriate technical and organizational measures to ensure a level of security for the data processing commensurate with the risk.
- *Data breach notification* – in case of a data breach (*i.e.*, "accidental and unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed"), the controller is required to notify[4] the competent supervisory authority[5] without undue delay (unless the data breach is unlikely to result in a risk to the rights and freedoms of data subjects) and, where possible, within 72 hours of discovering the breach.

---

4 The notification of the breach should describe at the minimum: (i) the nature of the breach, (ii) the likely consequences of the breach and (iii) the measures taken or proposed to be taken by the controller to address the breach or mitigate its possible adverse effects. The notification should also provide the name and contact details for the DPO or other contact person from whom information can be obtained.

5 The relevant supervisory authority is the supervisory authority with which a complaint has been lodged, the supervisory authority in the EU member state where the controller is established or, if the controller is not established in the European Union, the supervisory authority in the EU member state where the data subject affected by the processing resides.

- *Information and access for data subjects* – a controller is required to provide certain minimum information to a data subject at the time personal data is obtained. The data subject should be informed, among other things, about his/her rights with respect to the processing of his/her personal data, the purposes for which the personal data is processed, the categories of data recipients, the data retention period, as well as all instances when his/her data are transferred outside the European Union.

- *Rectification and erasure* – a controller must give a data subject an opportunity to correct and supplement personal data, or to erase the relevant data if certain conditions apply, such as when the data are no longer necessary for the purposes for which they were originally processed.

- *Record keeping* – a controller with 250 or more employees[6] must keep a record of all the processing activities (through documenting of all such activities, development and implementation of effective internal training programs and implementation of appropriate technical and organization safeguards) in order to demonstrate full compliance with the GDPR. The GDPR no longer requires the controller to give an advanced notice to relevant supervisory authorities of engaging in data processing.

- *Data protection officer and designated representative* – a controller may be required to appoint a data protection officer ("DPO") as specified by the GDPR[7] to be responsible for the controller's GDPR compliance and accountability. Additionally, a controller that is not established in the European Union but is subject to the GDPR may need to appoint a designated representative in the EU member state where the relevant EU data subjects reside, except in circumstances where the processing is occasional, does not involve large scale processing of specific categories of data and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purpose of processing.

Processors' obligations

The GDPR introduces the following key obligations for processors of personal data that did not exist under the old regime:

- *Data security* – a processor is required to implement appropriate measures to ensure adequate level of data protection;

---

6 Controllers with less than 250 employees are subject to record keeping requirements only if the processing (i) is likely to result in a risk to rights and freedoms of data subjects, (ii) is not occasional, or (iii) includes special categories of personal data, such as data relating to racial or ethnic origin, political opinions, religious beliefs or criminal convictions and offences.

7 A DPO is required to be appointed where the controller or processor is processing personal data as a public entity, or where the controller's or processor's core activities consist of processing operations that require large-scale, regular and systematic monitoring of data subjects or processing of sensitive data.

- *Data breach notification* – a processor is required to notify the controller of a data breach without undue delay;
- *Contractual relationship* – all processing of personal data by a processor on a controller's behalf must be done pursuant to a written, binding contract that must also be in electronic form;
- *Sub-processing* – a processor is required to obtain consent from a controller to delegate to another processor;
- *Record keeping* – a processor with 250 or more employees[8] is required to keep record of all data processing activities done on behalf of a controller containing specific information; and
- *Appointment of a DPO and designated representative* – the same requirements apply as in the case of controllers.

Transfer of data outside of the European Union

The GDPR allows for transfers of personal data out of the European Union when the data are being sent to a country that the European Commission (the "EC") has determined provides an adequate level of protection. The following countries have so far received an EC adequacy decision: Andorra, Argentina, Canada (commercial entities), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.

If a country is not considered to have adequate protections, such as the United States, then in order to transfer the personal data outside the European Union such country must fall within one of the derogations in the GDPR or the controllers and processors must provide adequate assurances that the personal data will be protected. The requirement for provision of adequate assurances applies not only to the initial third country transfer but must also be carried over for "onward transfers" down the chain.

Listed below are the various ways in which controllers and processors can provide adequate assurances of EU personal data protection. It is, however, important to note that in practice these adequate assurance mechanisms come with significant challenges and inherent difficulties for the transfer process, in addition to being time-consuming to implement. This, combined with the lack of clarity as to the ongoing viability or existence of these transfer mechanisms, adds to the complexity and uncertainty concerning the legality of personal data transfers from the European Union to third countries.

[8] Processors with less than 250 employees are required to comply with record keeping requirement only in specified circumstances as detailed in footnote 6 above.

- *2016 EU-U.S. Privacy Shield* – the Privacy Shield program negotiated between the European Union and the United States provides a mechanism that allows participating entities (*i.e.*, those subject to enforcement authority of the FTC or the U.S. Department of Transportation) to transfer EU personal data to the United States. The participating entities must self-certify compliance with the Privacy Shield by committing to process data only in accordance with the program's principles.

  The first annual review of the Privacy Shield, conducted in September 2017 by representatives of the EC, several European data protection authorities and their U.S. counterparts, resulted in a general endorsement of the mechanism, although some concerns were voiced regarding its long-term viability. While it is expected that some changes and updates to the Privacy Shield, in particular in the area of controls and safeguards, may come in the future, for the time being the Privacy Shield continues to be the easiest method for U.S. entities to comply with the EU requirements on transfer of personal data out of the European Union.

- *Standard data protection clauses* – these contractual clauses, which must be approved by the EC, need to be embedded in contracts between data controllers and processors. They provide means for the parties to guarantee an adequate level of protection for the personal data being processed in satisfaction of the GDPR requirements.

- *Binding corporate rules* – these 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.

- *Codes of conduct and certifications* – compliance with the GDPR may also be demonstrated through codes of conduct (prepared and approved by associations or bodies representing controllers and processors) and certification mechanisms, seals or marks (established by supervisory authorities).

U.S. rulings and subpoenas requiring production of EU personal data

Under Article 48 of the GDPR, 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 mutual legal assistance agreement (MLAA). The United States and the European Union have entered into a binding MLAA; nevertheless, Article 48 may be problematic when there are conflicts between U.S. legal process and the MLAA.

Additionally, as relates to data transfers from the European Union to third countries, in the absence of a decision on adequacy or safeguards in the form of adequate assurances discussed above, Article 49 provides several derogations that would allow for such transfers. In context of U.S.-based litigation (but also regulatory investigations and corporate transactional work) and related cross-border e-discovery practices, it may be possible to rely on one such derogation that allows the transfer to the third country if such transfer "is necessary for the establishment, exercise or defence of legal claims."

Penalties for noncompliance with the GDPR

The GDPR revises the EU compliance mechanism for data privacy laws and imposes significantly increased penalties for failure to comply with its requirements. Under the GDPR rules, the fines for noncompliance are up to the greater of €20 million or 4% of the entity's worldwide annual turnover. A noncomplying entity risks facing action from both the relevant supervisory authority, which may result in not just fines, but also enforcement orders (designed to block noncompliant entities from accessing the EU markets) and other sanctions, as well as from individuals, which may result in damage claims. Even if fines and other penalties are not ultimately imposed, simply being investigated for potential GDPR violations and having to comply with a supervisory authority's requests to produce records documenting compliance could be burdensome and costly for the affected entity.

Conclusion

Given the expanded reach and complexity of the GDPR, it is clear that a number of non-EU entities that were previously outside the scope of the EU data privacy laws will now fall within its purview. This risk, combined with the significantly increased penalties and the fast approaching effective date of the GDPR, highlights the importance of early and proper determination of its applicability. We can expect, given the expansion of coverage under the GDPR, as affected entities focus on the practical implications of the new privacy rules, that significant interpretive questions will arise and will need to be addressed, including as to the scope of coverage of the data of natural persons outside the European Union for those that have established controllers or processors in the European Union.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Mark S. Bergman
+44-20-7367-1601
mbergman@paulweiss.com

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Jeh Charles Johnson
+1-212-373-3093
jjohnson@paulweiss.com

Lorin L. Reisner
+1-212-373-3250
lreisner@paulweiss.com

Richard C. Tarlowe
+1-212-373-3035
rtarlowe@paulweiss.com

Daniel J. Toal
+1-212-373-3869
dtoal@paulweiss.com

John J. Satory
+44-20-7367-1606
jsatory@paulweiss.com

E-Discovery counsel Ross M. Gotler and Securities practice management attorney Monika G. Kislowska contributed to this Client Memorandum.