Client Alert
May 22, 2018

New European Rules for Personal Data Have Global Reach

By Daniel Appelman

On May 25, 2018, the European Union's General Data Protection Regulation (the "GDPR") will become effective and will subject all companies world-wide that collect personal data from EU residents to new data privacy requirements.

I. What Is The GDPR?

The GDPR is a framework of regulations that govern the collection, processing, use and protection of information relating to EU residents. (Such information is referred to herein as "***Personal Data***", and the EU residents to whom such Personal Data relates are referred to herein as "***Data Subjects***".) GDPR compliance is required of all companies that collect Personal Data from EU residents, including companies located outside the EU. In this sense, the GDPR has extraterritorial reach.

Personal Data can include the following categories of personally identifying information: (i) basic identity information such as name, address and ID numbers, (ii) web data such as location, IP address, cookie data and RFID tags, (iii) health and genetic data, (iv) biometric data, (v) racial or ethnic data, (vi) political opinions and (vii) sexual orientation. Personal Data can also include so-called "pseudonymized" data, i.e., data that results from the replacement of certain fields in the data set with artificial identifiers such as unique numbers to render the data record less personally identifying, if the process of replacement can be reversed.

II. The Goals of the GDPR

The GDPR was drafted with two goals in mind: (1) to harmonize the EU's data protection laws to reduce compliance burdens on those who control and process Personal Data ("***Controllers***" and "***Processors***" respectively) and (2) to refresh and adapt Data Subjects' rights in their Personal Data to new technological challenges and capabilities.

A. Harmonization

The GDPR accomplishes the first of its two goals (to harmonize the EU's data protection laws to reduce compliance burdens on Controllers and Processors) by replacing the EU's current Data Protection Directive ("***DPD***") with a unified, legally-binding set of regulations for all of the EU.

Under the DPD, each Member State interpreted and enforced a general set of data protection guidelines, and enforcement actions could be brought against Controllers and Processors in any Member State. Each Member State interpreted and enforced the DPD's guidelines differently. This led to significant legal uncertainty and variability for Controllers and Processors across the EU. In contrast, the GDPR provides a single set of legally binding rules that Member States cannot materially alter and that can only be enforced against any particular Controller or Processor by a single "***Supervisory Authority***".[1]

B. Expanding Data Privacy Rights for Data Subjects.

The GDPR attempts to accomplish its second goal (to safeguard Data Subjects' "fundamental right" to the protection of their Personal Data) by providing new

For more information on privacy law, please contact Daniel Appelman at 650.331.7014 or dappelman@mh-llp.com

rights for Data Subjects. These new rights allow Data Subjects to control the collection and use of their Personal Data and how, and under what circumstances, it can be retained. The GDPR also imposes significant new requirements on Controllers and Processors that implement those new rights and the GDPR's fundamental data protection principles. And the GDPR provides for significant fines in the event that Controllers or Processors fail to comply with those new requirements.

(i) The GDPR provides substantial new rights to Data Subjects so they can control their Personal Data.

The GDPR provides a variety of new rights for Data Subjects that improve their ability to control their Personal Data, many of which will impose new costs on Controllers and Processors. For example, under the GDPR Data Subjects have the right to demand to know what data companies possess about them and what those companies do with that information. Companies must comply within one month of each such request. Data Subjects have the right to ask for correction, object to processing, lodge a complaint, or even ask for the transfer of their Personal Data. And Data Subjects have the right to revoke their consent to have their data processed.[2]

The new regulation provides a right to "data portability" that requires Controllers to provide a copy of a Data Subject's Personal Data upon request. It also gives individuals the power to have their Personal Data erased in some circumstances. Those circumstances include (i) when the possession of that data is no longer necessary for the purpose for which it was collected, (ii) when the consent of the Data Subject has been withdrawn, (iii) when there's no legitimate interest in continuing to possess or process it, and (iv) when it has been unlawfully processed.

(ii) The GDPR imposes significant new requirements on Controllers and Processors.

The GDPR requires that Personal Data be (i) processed lawfully, fairly and in a transparent manner in relation to the Data Subject, (ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, (iii) limited to what is necessary [for] the purposes for which they are processed, (iv) accurate and … kept up to date, (v) kept in a form which permits identification of Data Subjects for no longer than is necessary, and (vi) processed in a manner that ensures appropriate security of the Personal Data.

The GDPR expands on these requirements by imposing a long list of specific obligations on Controllers and Processors. Article 6 provides a list of situations in which the processing of Personal Data is done "lawfully", including with the Data Subject's consent. Article 9 prohibits processing of "special categories of Personal Data" that are particularly sensitive or deserving of protection, except in certain situations.[3] Controllers and Processors must also implement "privacy by design" and take proactive steps to adopt adequate data security policies and practices. If there are any data breach incidents, Controllers and Processors must comply with stringent data breach notification procedures.[4] Controllers and Processors must "rectify" and correct inaccurate Personal Data, delete Personal Data upon a Data Subject's request "without undue delay" and keep certain records and be able to prove that they have complied with other duties under the GDPR. In some cases, Controllers and Processors must conduct data protection impact assessments. Any Controller or Processor that is not established in the EU must designate a representative in the EU to receive enforcement and other legal notices, except in certain circumstances.[5]

(iii) The GDPR provides for substantial fines if its compliance requirements are breached.

The GDPR provides for potential fines for each violation of up to four percent (4%) of a company's worldwide turnover (total revenues) for the preceding year or €20 million (almost US$24 million), *whichever is higher*. Until a track record of enforcement is established, it is difficult to predict whether and under what circumstances the maximum fines will be levied, or what the typical fines will be for noncompliance.

III. Transferring Personal Information from the EU to the US

The GDPR makes it unlawful to transfer Personal Data out of the EU unless (i) the EU European Commission determines that the receiving jurisdiction "ensures an adequate level of protection" consistent with the GDPR; (ii) the processing entity has provided "appropriate safeguards"; or (iii) the individual Data Subject has provided specific consent for the transfer. Companies that collect Personal Data from EU residents and transfer that Personal Data to servers located in the U.S. are violating the GDPR unless they can demonstrate adherence to one of the aforementioned alternatives. Many companies in the U.S. avail themselves of the "safe harbor" provided through self-certification procedures under the EU-U.S. Privacy Shield Framework.[6]

We recommend that our clients determine whether they are transferring Personal Data from the EU to the U.S. If your company is transferring Personal Data from the EU to the U.S. and it is impractical to obtain the consent of the Data Subjects for those transfers, you should consider adopting the data protection practices required by the Privacy Shield Framework.

IV. Does the GDPR Apply to My Company?

The GDPR applies to companies that collect Personal Data from EU users who access their websites, applications and services. It also applies to companies that hire employees or contractors who reside in the EU. In both cases those who control and process that data must be within both the territorial and material scope of the GDPR in order to be subject to its terms.

A. Territorial scope of the GDPR

The GDPR's territorial scope of coverage includes all Controllers and Processors that are established[7] in the EU. Controllers and Processors that are *not* established in the EU are also within the GDPR's territorial scope if they collect and/or process Personal Data of any EU resident (i) in connection with offering goods or services in the EU, or (ii) as a result of monitoring the behavior of any EU resident which takes place in the EU, including through cookies and other online tracking tools.

It is an open question whether the mere accessibility of a company's website, email address or other contact details by EU residents constitutes offering that company's goods or services in the EU. Recital 23 of the GDPR suggests that it isn't. However, the language of that recital is ambiguous and will only be clarified by future regulatory and judicial interpretation.

We recommend that our clients determine whether they have, or plan to have, users or customers in the EU to which they market their goods or services or whether they track or monitor the behavior of any Data Subjects through Personal Data collected using cookies or another automated data collection tool. Unless the answer to both questions is "no", then your company is probably within the territorial scope of the GDPR.

B. Material scope of the GDPR

Article 2 of the GDPR states that the GDPR "applies to the processing of Personal Data wholly or partly by automated means and to the processing other than by automated means of Personal Data which form part of a filing system or are intended to form part of a filing system." The GDPR does not define "automated processing", so it is not clear what methods of processing will be deemed automated under the GDPR. It is also not clear under the GDPR what does and does not constitute a filing system; but a conservative interpretation would conclude that employee records (payroll, etc.) *do* constitute a filing system.

We recommend that our clients determine whether they processes (including through a third party data processor) information about EU residents that may include Personal Data, and if so, whether that processing (including by a third party) is done "by automated means" or "as part of a filing system". If your company (or its third party data processing contractor) processes Personal Data by automated means or as part of a filing system, then your company is most likely within the material scope of the GDPR.

V. Conclusion

The GDPR imposes significant new requirements on Controllers and Processors in the EU and those outside the EU who market or sell goods or services in the EU or track the behavior of Data Subjects. Each client should evaluate its data collection and use practices to determine whether its practices bring the client within the territorial and material scope of the GDPR. In such event, we would recommend taking steps to develop a detailed program that provides a step-by-step plan for ensuring compliance.

The GDPR contains 99 articles setting out the rights of individuals and obligations placed on organizations covered by the regulation. This client alert is not intended to be a complete description of all of those rights and obligations. *We recommend that our clients familiarize themselves with the requirements of the GDPR, assess which of them apply to their companies, and institute a compliance program.*

Read the full text of the GDPR

1) Each Member State will still have a body that enforces the GDPR, but only against Controllers and Processors for which it is the Supervisory Authority.

2) GDPR, Article 17. This is the so-called "right to be forgotten".

3) GDPR, Article 9(1) ("Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.").

4) GDPR, Article 33(1). In most cases, Controllers must inform Data Subjects of any data breach involving their Personal Data within 72 hours after learning of the breach.

5) GDPR, Article 27(2) (a Controller or Processor does not need an EU representative if its processing of EU residents' Personal Data is "occasional, does not include, on a large scale, processing of special 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 purposes of the processing").

6) The EU-U.S. Privacy Shield Framework became effective as an option in June 2016 and is consistent with the GDPR. However, it is currently under challenge in the EU and prospects for its continued availability are uncertain.

7) It is not clear at this time what "establishment" means in the GDPR. This memorandum assumes that it means establishment of an office or other non-temporary place of business.