MorrisonCohen LLP
Law Firm to the Middle Market®

Client Alert

US-Based Organizations Must Prepare for Imminent Implementation of European General Data Protection Regulation

May 7, 2018 – Beginning May 25, 2018, any entity (even ones lacking any physical presence in the European Union) that offers goods or services to any EU "data subjects" (i.e., natural persons), whether or not requiring any payment, or monitors the behavior of data subjects within the EU, and processes or holds personal data of those data subjects is required to comply with the General Data Protection Regulation ("GDPR").

Personal data under the GDPR is broader than the comparable US concept of "personally identifiable information", and includes information like name, identification number, location data, online identifiers, and one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person in question.

The GDPR is applicable to both "data controllers," (i.e., the persons who determine the purposes and means of the processing of personal data), and "data processors," (i.e., the persons who process personal data on behalf of the data controller).

Compliance with GDPR requires organizations to make certain operational changes, including:

a. Collection of Personal Data – Under the GDPR, personal data may only be collected for a specified, explicit and legitimate purpose and must be processed lawfully, fairly and in a transparent manner. Additionally, collection and use of personal data needs to be limited to the purpose it was collected for, should always be accurate, and should not be stored for longer than necessary. The data controller or data processor must enable the data subject to rectify any inaccurate data as well as exercise his or her right to be forgotten where the personal data is not being used for the purpose it was collected. The data controller must also provide the data subject with its identity and contact details, purposes of processing the personal data, and information relating to third party use or transfers of personal data.

b. Consent or other Legal Basis – Unless an organization falls under one of five permissible lawful bases for collection, organizations must receive the express consent of an individual before processing his/her personal data. This consent must be freely given, specific, informed and unambiguous and is valid only for the specific purpose it was given. If the data controller intends to use the personal data for an unconnected new

purpose, consent must be requested – and received - again. The data subject has the authority to withdraw consent at any time. The other legal bases for data collection are:

a. To facilitate performance of a contractual obligation owed to the data subject;

b. To comply with a legal obligation to which the data controller is subject;

c. To protect the vital interests of a natural person;

d. To perform a task necessary for the public interest;

e. To pursue the legitimate interests of the data controller or other third party unless contrary to the rights and freedoms of the data subject.

c. Engaging Data Processors – If any organization, in its capacity as a data controller, engages a data processor to process personal data on its behalf, the data controller must enter into a binding written contract with the data processor that guarantees the data processor will implement appropriate technical and organizational measures to ensure GDPR compliance.

d. Security Measures – Organizations required to comply with the GDPR must implement appropriate technical and organizational measures to ensure security of personal data including pseudonymization and encryption of personal data, maintaining and testing disaster recovery and back-up mechanisms, conducting employee training, and ensuring confidentiality, integrity and resilience of processing systems and services.

e. Breach Notification – The GDPR requires data controllers to notify the appropriate EU supervisory authority of the personal data breach, without undue delay, and where feasible, within 72 hours of becoming aware of the breach, unless it is likely to result in a risk to the rights and freedoms of natural persons. If the notification is not made within 72 hours, it must be accompanied by reasons for the delay. The data controllers are also required to document any personal data breaches, including facts relating to the breach, its effects, and the remedial action taken. In addition, data processors are required to notify the data controller, without undue delay, after becoming aware of a personal data breach. When notifying the appropriate supervisory authority, the data controller is required to, at least, describe the nature of the personal data breach, communicate the name and contact details of the data protection officer or such other contact person, describe the likely consequences of the breach, and describe the mitigating measures taken or proposed by the data controller.

The potential penalties for non-compliance will depend on the degree and nature of culpability of the party, and can include administrative fines of up to 20 million euros, or in the case of an undertaking (i.e., any entity engaged in economic activity), up to 4% of its total worldwide annual sales for the preceding fiscal year, whichever is higher. Therefore, it is imperative for organizations fully to understand their interaction with EU data subjects and their business operations with the EU, to have defined processes in place to understand the personal data they hold, to collect personal data only for limited purposes and for limited time periods, with adequate consent or other legal basis, to ensure that they, along with their vendors and third party processors, have adequate security measures in place, and have policies and procedures to deal

with a suspected breach and to enable data subjects to correct, delete or migrate data out of the possession and control of the data controller or data processor.

For additional assistance or information regarding the GDPR or other matters concerning data privacy and security, please contact your regular attorney here at Morrison Cohen, or any of following:

David Lerner
(212) 735-8609
dlerner@morrisoncohen.com

Jessica L. Lipson
(212) 735-8683
jlipson@morrisoncohen.com

Shruti Chopra
(212) 735-8628
schopra@morrisoncohen.com