Client Alert March 2018

New European Data Protection Regulation: What does it mean for U.S. Businesses?

If your business maintains personal data on EU-based individuals – whether customers, clients, employees, suppliers or users of your technology, you will need to comply with the EU's new data protection regulation, the GDPR, effective **May 25, 2018**.

The General Data Protection Regulation ("GDPR") will govern how businesses process "personal data" relating to an EU resident. Personal data encompasses information such as a person's name, email address, IP address, etc. – anything that could identify an individual. The GDPR will widely define the term "process" to include storing, using, disclosing, transferring and erasing data.

Any business – whether based in the U.S. or Europe – that processes the personal data of EU residents when offering goods or services to the EU, or when monitoring an EU resident's online behavior, will need to comply with the GDPR. The GDPR will apply to businesses that determine the purpose and means of processing personal data ("*Data Controllers*") and to businesses that process personal data on behalf of Data Controllers ("*Data Processors*").

Penalties for a ***serious breach of the GDPR may result in a fine of up to €20 million (~ US$25 million) or 4% of global revenue***, whichever is higher. EU residents will also have a direct right to sue for damages in EU member-state courts.

Personal Data in the EU

Outside Europe, businesses often view personal data they hold as their property – theirs to process, store, provide, or even sell to a third party. With the incoming regulation, the EU, by contrast, will view any data from which an individual can be identified as the property of that individual. A business may hold an individual's personal data for a particular purpose or transaction, but solely on a temporary or voluntary basis: the individual will retain ultimate ownership and control over his or her personal data, subject only to limited exceptions provided by law. The GDPR shall also provide for an individual's "right to know" how businesses store, use, and process their personal data and enables them to demand businesses delete their personal data upon request.

What do U.S. businesses need to do?

U.S. businesses will need to take steps to identify whether they process the personal data of EU residents, for example, their clients and employees. If so, they must determine

whether they are a Data Controller or Data Processor and take steps to ensure that they will be compliant with the GDPR by May 25, 2018.

Key changes under the GDPR include:

- **Expanded extraterritorial reach** – the GDPR will apply to non-EU businesses that process the personal data of EU residents when offering goods or services to them, or that monitor the behavior of EU residents;

- **Transfers of personal data outside the EU** – the European Commission has a list of adequate non-EU countries to which EU data can be transferred. The EU-U.S. Privacy Shield is on this list. U.S. businesses will therefore need to comply with an approved form of and procedure for transfer, such as the privacy shield requirements, to receive EU data transfers;

- **Relying on consent to process data** – consent will remain a lawful basis for processing data under the GDPR, but must be (a) separate from other terms and conditions, (b) freely given, (c) informed, and (d) unambiguous. Consent cannot be inferred from silence or a pre-ticked box. There must also be a simple way to withdraw consent;

- **Data Controllers will have a direct legal obligation to give effect to the rights of EU residents** – they will be obligated to inform EU residents of their rights (including the rights of erasure and data portability);

- **Accountability of Data Controllers** – they will have a responsibility to implement appropriate technical and organizational measures to ensure GDPR compliance (e.g., encryption), and to demonstrate compliance;

- **Data Processors will now be directly regulated** – they will be subject to fines;

- **Maintaining written records** – Data Controllers and Data Processors will be required to keep written records of all processing activities and disclose these records to the relevant supervisory authority on request;

- **Contracts between Data Controllers and Data Processors** – Data Controllers will need a contract with Data Processors, which must include certain provisions specified in the GDPR; and

- **Mandatory 72-hour reporting obligation of a data breach** – data breach reporting obligations will include notifying the relevant supervisory authority of a breach within 72 hours of breach detection.

About Curtis

Curtis, Mallet-Prevost, Colt & Mosle LLP is a leading international law firm. Headquartered in New York, Curtis has 17 offices in the United States, Latin America, Europe, the Middle East and Asia. Curtis represents a wide range of clients, including multinational corporations and financial institutions, governments and state-owned companies, money managers, sovereign wealth funds, family-owned businesses, individuals and entrepreneurs.

For more information about Curtis, please visit www.curtis.com.

Attorney advertising - The material contained in this Client Alert is only a general review of the subjects covered and does not constitute legal advice. No legal or business decision should be based on its contents.

Please feel free to contact any of the persons listed below if you have any questions on this important development:

Jonathan Walsh
Partner
jwalsh@curtis.com
New York: +1 212 696 8817

Winta Jarvis
Partner
wjarvis@curtis.com
London: +44 20 7710 9830

Edward Combs
Associate
ecombs@curtis.com
New York: +1 212 696 6069

Daniel Banaszynski
Associate
dbanaszynski@curtis.com
New York: +1 212 696 6153