New York Law Journal

The EU General Data Protection Regulation: Why It Matters Here

By Anthony E. Davis and Steven M. Puiszis
New York Law Journal
May 4, 2018

As published on Page 3

The EU General Data Privacy Regulation (GDPR) goes into effect on May 25, 2018. It establishes a uniform data privacy law across the EU. The right to data privacy is considered a fundamental human right in the EU, and the GDPR reflects that approach. Law firms do not need to have an office in the EU or even set foot in the EU to be subject to the GDPR. The GDPR applies to any type of business, wherever it is located, that either: (1) offers goods or services in the EU; or (2) monitors the behavior of EU citizens. If a law firm offers its services in the EU, and has personal information about residents of the EU, it is subject to the Regulation even in the absence of any other connection with the EU. The size of the law firm (or other business) makes no difference.

Penalties for noncompliance with the GDPR are potentially significant. They can range up to the greater of £20 million or 4 percent of an entity's annual worldwide turnover for serious violations. Actions can also be brought by data subjects or on their behalf in their country of residence for an infringement of his/her/their privacy rights.

The GDPR focuses on the privacy and security of personal data in connection with virtually any activity that can be performed in connection with personal data, including collecting, using, storing, selling, sharing or transmitting it. And what is considered personal information is far broader in the EU than the United States. Personal information encompassed by the GDPR is essentially anything that can be used to identify a natural person, including contact information and even a computer's IP address.

The GDPR requires "data subjects" to be given clear and transparent notice of the ways in which, and the purposes for which their personal data is processed and provides a number of rights to data subjects concerning their personal information, including:

- To be informed about the personal data being held and processed;
- To be told about the purposes for which the data is being processed and the lawful basis for processing that data including any "legitimate interest" pursued by the controller;
- To be told about the period of time the data will be retained;
- To access their personal data, complete incomplete information, to correct information, delete personal data and transfer data;
- To object to the processing of their personal data or to restrict the processing of it;

The GDPR requires extensive record keeping and documentation to demonstrate compliance with its requirements.

Territorial Reach

The GDPR applies to any organization or entity "established" in the EU that processes personal data in connection with the activities of that entity, regardless of where the processing takes place. Factors that can trigger the GDPR include the offering of goods or services in a member state's native language, pricing goods or services in the currency used in that member state, or the reference to other customers in a member state, the international nature of a product or activity offered, or a website's use of a top-level EU domain extension (e.g., www.IWantYourBusiness.uk).

Personal Data

Personal data is defined as "any information relating to an identified or identifiable natural person," a "data subject," that can be used to "directly or indirectly" identify the person "by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of the natural person."

Data Processors and Controllers

The GDPR imposes requirements upon data "processors" and "controllers." A processer is defined as "a natural or legal person, public authority or agency, or any other body which processes personal data on behalf of the controller." A controller is a "natural or legal person, public authority, agency or other body which either alone or jointly with others, determines the purposes and means" by which personal data will be processed.

The GDPR imposes security requirements on controllers and processors to protect personal data against unauthorized or unlawful access, acquisition, disclosure or processing, and against unlawful or accidental loss, destruction, alteration or damage to that data, and requires they keep records of their processing activities and be prepared to demonstrate compliance with the GDPR's data protection principles.

Controllers must use only processors that can meet the requirements of the GDPR and must have a written agreement with the processor aimed at achieving that compliance.

Data Processing Requirements

A controller must have at least one lawful basis for the processing of EU personal data, which could include the data subject's consent, or processing necessary for the performance of a contract, for compliance with a legal obligation, for a legitimate interest pursued by the controller or to protect the vital interests of the data subject or another natural person. Personal data can only be collected for specific, explicit and legitimate purposes and for no longer than is necessary for the purposes for which it was processed. Information collected for one purpose cannot be used or processed in a manner that is incompatible with that purpose.

Personal data should be accurate and must be kept up to date. Data subjects have the right to review, correct and/or demand that their personal data be corrected or erased without reasonable delay, generally within 30 days.

Sensitive personal data, which is separately defined, may only be processed in narrowly defined and limited circumstances, which are set out in detail in the Regulation.

Lawful Basis for Processing

Consent of the data subject is a lawful basis for processing his or her personal data, but to be valid, the consent must be specific, explicit, informed and freely given. Consent cannot be assumed by silence or a nonresponse. Opt in consent is required. The burden of demonstrating consent to the processing activity rests on the controller.

A data subject must be provided with the ability to withdraw his or her consent at any time.

EU Representative

Controllers or processors outside the EU are required to appoint a representative in the EU as a point of contact for data subjects and supervisory authorities unless the processing is occasional, and does not involve large scale processing of sensitive personal data.

Cross-Border Data Transfers

Except in limited circumstances specified by the Regulation, personal data cannot be transferred outside of the European Economic Area unless the GDPR's requirements are met to a country the European Commission has determined provides an adequate level of protection to personal data. The United States does not qualify; however, transfers are permitted under the EU-U.S. privacy shield regime, which involves a self-certification process for U.S. organizations.

Breach Notification

The GDPR requires controllers to report a personal data breach to the relevant supervisory authorities "without undue delay, and where feasible, no later than 72 hours" of learning of the breach. A Processor must notify a Controller of a personal data breach without undue delay after becoming aware of the breach.

Steps Law Firms Need to Take Now

- Determine if the GDPR applies to your firm.
- If so, identify all EU personal data in your possession.
- Determine if you possess "sensitive" personal data.
- Identify all locations where EU personal data is stored or processed.
- Evaluate the risks to the security of EU personal data at each location.
- Identify all processing activities you perform or that are performed on your behalf.
- Establish and document that at least one (preferably more) lawful basis exists for each processing activity.
- Evaluate/update privacy notices on your website to address GDPR's requirements and draft privacy notices explaining data subjects' rights under the GDPR for letters and/or forms going forward. Also obtain pop up consent for the use of cookies on your website.
- Identify and document the lawful basis for any EU –US cross border data transfers.
- Review all third-party agreements with any entity that does anything with EU personal data and modify or amend to ensure the GDPR requirements are met.
- Evaluate your system's capability to permit timely access, correction, and erasure of any EU personal data.
- Develop a recordkeeping system to document and establish compliance.
- Prepare any necessary breach response templates.
- Evaluate if you need to designate a personal representative in the EU and/or a data protection officer.
- If you rely on consent, evaluate how the consent is obtained.
- If your entity operates in more than one EU member state, consider evaluating if you should designate a "main establishment" and who will be the lead data protection supervisory authority.
- Consider whether you need to put procedures in place to verify the ages of individuals and/or obtain parental or guardian consent to data processing activities of anyone under the age of 16 in the EU or 13 in the United States.
- Consider the possibility of anonymizing/pseudonymizing personal data.
- Prepare policies, procedures and processes for conducting data protection impact assessments.
- Select only vendors that can meet the GDPR requirements going forward.

As noted at the outset, firms that have any personal information about any EU citizens must prepare to address the requirements of the Regulation before May 25, 2018.

Anthony E. Davis *and* ***Steven M. Puiszis*** *are partners of Hinshaw & Culbertson. Anthony E. Davis is a past president of the Association of Professional Responsibility Lawyers. Steven M. Puiszis is Hinshaw's General Counsel—Privacy, Security & Compliance.*