As Seen In the March 26, 2018 issue of
BUFFALO Law Journal

Prepping for the GDPR deadline

The GDPR compliance deadline of May 25 is looming, but there is still time to take steps to comply.

GUEST COLUMN

JENNIFER BECKAGE

What is the GDPR?

General Data Protection Regulation is a data privacy regulation intended primarily to protect a very broad set of personal data belonging to individuals in the European Union. The GDPR applies to the 28 EU member states, plus Norway, Ireland and Lichtenstein. Under the GDPR, personal data includes, but is not limited to, an individual's name, address, email address, IP address, Social Security number, biometric data, location data, online identifiers and other information (personal data). The GDPR identifies specific requirements organizations subject to the GDPR must take to protect personal data. Beginning May 25, organizations must comply with the GDPR's requirements or risk being assessed penalties for noncompliance.

To whom does it apply?

The GDPR generally applies to any organization that controls or processes personal data, regardless of where the organization is located. Organizations in the United States may be subject to the GDPR even if they have no physical presence in the EU. The GDPR takes a global approach to privacy and provides data subjects control over the manner in which their personal data is obtained, used, shared and stored. The regulation is based on the principle that individuals have a fundamental right to maintain privacy.

What are the core principles of the GDPR?

The GDPR provides a construct under which personal data is either controlled or processed. A controller typically obtains or collects personal data and determines the purposes and means of processing the information. A processor handles such personal data. For example, a business is a controller of a customer's personal data, but a cloud storage vendor may store the data on behalf of the controller. Both controllers and processors are required to comply with the GDPR.

Under the GDPR, organizations that have access to personal data must have a legal basis for obtaining, controlling or processing it – e.g., consent. Thus, in many cases it will be necessary for an organization to obtain a data subject's clear, unambiguous and affirmative consent in order to collect, use, hold or transfer personal data or have another basis for having it. However, pursuant to the new regulation, some "sensitive data," such as a person's political opinions or sexual orientation, cannot be collected absent specific grounds for doing so.

The GDPR recognizes various "rights" of EU data subjects. For example, GDPR provides data subjects the "right to be forgotten" and to withdraw their consent for an organization's use of their personal data. This will require organizations to develop processes for addressing and complying with such requests when circumstances warrant.

The GDPR also imposes obligations on data controllers and processors in the event of a data breach. For example, one such obligation is that if there is a personal data breach, as defined under the regulation, the supervisory authority must be notified "without undue delay" and "no later than 72 hours," unless the event is "unlikely to result in a risk to rights and freedoms of natural persons."

What to do?

If your organization is subject to the GDPR, there are a number of steps that the organization can take between now and May 25 to work toward compliance with the regulation. First, conduct an inventory of existing data and identify that which may be subject to the GDPR. Next, develop a means to either obtain the data subject's consent to have and use the personal data or establish a legal basis for holding on to it. For new personal data that your organization obtains in the future, provide appropriate disclosures regarding the information collected and an accurate description of how such data will be used and by whom. It is important to document any and all actions taken to comply with the GDPR. Work closely with your organization's information technology professionals to develop policies and procedures for honoring a data subject's fundamental rights to access and erasure of personal data. Finally, if your organization has not yet developed a data incident response plan, the GDPR contains obligations that will apply to the personal data, so use this opportunity to develop a robust incident response plan for your organization.

Enforcement and sanctions for noncompliance

The GDPR provides for fines of up to $20 million EUR, or 4 percent of an organization's worldwide annual turnover, whichever is greater. Plus there may be other penalties, criminal charges and/or civil liability. It remains to be seen how the GDPR will be enforced.

There is still time before May 25 to work toward compliance with the GDPR, but an organization should not wait too much longer to determine if the GDPR applies.

JENNIFER BECKAGE is team leader of the Data Security & Privacy Practice at Phillips Lytle LLP: jbeckage@phillipslytle.com