New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Cybersecurity

WWW.NYLJ.COM

VOLUME 259—NO. 42

MONDAY, MARCH 5, 2018

The GDPR: A Silver Lining For Data Governance

BY JESSICA B. LEE

SHUTTERSTOCK

The countdown to the enforcement date of the EU General Data Protection Regulation (GDPR) has begun and it's becoming increasingly clear that many U.S. organizations are poised to be caught in its crosshairs. Organizations that offer goods or services in the EU (whether or not a payment is involved) or that monitor the behavior of individuals in the EU, will be subject to the GDPR's requirements whether or not they have a presence in the EU. For U.S. organizations that are being exposed to the EU's regulatory regime for the first time, panic may be setting in (if it hasn't already). Requirements around honoring expanded data subject rights, maintaining records of processing, documenting the legal basis for such processing, and complying with the new security breach notification requirements, among others, may be particularly challenging for organizations that don't have well–developed data governance policies or centralized systems and databases.

The GDPR replaces the previous Data Protection Directive 95/46/EC (the Directive) as the governing privacy regulation in the EU. While key principles of data privacy addressed in the Directive remain largely the same, there are some significant policy changes, and, as a result, a fair amount of uncertainty about how the regulation will be enforced. With reports suggesting that many organizations won't be "fully compliant" by May 25, 2018 (the GDPR's enforcement date), the next year or two may prove instructive as the first round of enforcement begins.

Although some will find this uncertainty frustrating, there may be a silver lining. Where the Directive included an obligation to notify supervisory authorities about an organization's processing activities, the GDPR allows organizations to document their own processing activities, determine if they are compliant with the specific

JESSICA B. LEE *is a partner in the advanced media and technology practice at Loeb & Loeb.*

requirements, identify and mitigate any risks created by their data use, and ultimately hold themselves accountable for compliance. This emphasis on accountability and record keeping may actually help create the safety net needed to navigate the GDPR's grey areas. Organizations with a robust data governance program, that have a documented and considered approach to GDPR compliance, are much less likely to be at the front lines of GDPR enforcement, and certainly should not be subject to the highest fines (up to $20 million or 4 percent of global annual turnover).

GDPR: Accountability For Risk-Based Approach

Article 5(2) of the GDPR introduces the accountability principle, which requires organizations that control the processing of personal data ("controllers") to demonstrate (read: document) compliance with the GDPR's principles relating to the processing of personal data (i.e., lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; and integrity and confidentiality). This notion of accountability is not new; it was included as a basic data protection principle in the OECD Guidelines in 1980 (and the most recent update in 2013) and has been incorporated in various forms in other international privacy regulations. However, previous iterations of the accountability principle were centered on assigning responsibility or fault for failures in privacy compliance. Under the GDPR, accountability is recast as an obligation to establish a systematic and ongoing approach to privacy. In effect, it codifies the obligation to create a data governance program that incorporates the principle of privacy by design, using tools like privacy impact assessments to routinize data protection within an organization. More than just a mandate to create policy documents, the GDPR creates a regulatory environment under which privacy and data governance are forced to become a standard element of an organization's operations.

The GDPR replaces the previous Data Protection Directive 95/46/EC as the governing privacy regulation in the EU.

This principle of accountability must be viewed in the context of the GDPR's risk-based approach to privacy. Under Article 24 of the GDPR, controllers are required to assess the nature, scope, context and purpose of processing, and based on the risks presented: (1) implement appropriate technical and organizational measures to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR; and (2) review and update those measures where necessary. Organizations are directed to take into account "the state of the art and the costs of implementation" and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons." The GDPR provides suggestions (although no mandates) for which measures might be considered "appropriate to the risk." The pseudonymization and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and the creation of a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing will provide a good start for organizations to start mapping out their compliance efforts.

DPIAs. Historically, national data protection authorities in Europe (DPAs) have recommended privacy impact assessments (PIAs), tools used to identify and mitigate privacy risks during the design-phase of a project, as an element of privacy by design. Under Article 35 of the GDPR, data protection impact assessments (DPIAs)—a more robust version of the PIA—are now mandatory when an organization is engaging in activities that pose a high risk to an individual's rights and freedoms. The DPIA presents an opportunity to demonstrate that safeguards have (hopefully) been integrated into an organization's data processing activities and that

the risks presented by a processing activity have been sufficiently mitigated

While the risks analysis itself is largely left in the hands of each organization, determinations that are wildly off-base may not be defensible. However, if an organization can justify its position, relying on industry practice or other guidance, even if regulators ultimately determine that additional measures were required, it may be able to avoid significant fines. Notably, the failure to complete a DPIA itself could result in fines of up to 10 million Euros or up to 2 percent of the total worldwide turnover of the preceding year.

Records of Processing. Under the Directive, organizations were obligated to notify and register processing activities with local DPAs. The GDPR eliminates this requirement and instead puts the burden on both controllers and processors to maintain an internal record of processing activities, which must be made available to DPAs upon request. These records must contain all of the following information: (1) the name and contact details of the controller and where applicable, the data protection office; (2) the purposes of the processing; (3) a description of the categories of data subjects and of the categories of personal data; (4) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations; (5) the transfers of personal data to a third country or an international organization, including the documentation of suitable safeguards; (6) the envisaged time limits for erasure of the different categories of data; and (7) a general description of the applied technical and organizational security measures. Where processing activities take place across a variety of disconnected business units, organizing these records may be challenging. Organizations will need to audit each of their business units and their corresponding systems and processes to determine their processing activities and consider moving to a more centralized system.

Next Steps: Preparing For May 25th and Beyond

Between now and May 25th, organizations should be focused on creating the processes and documents that will help tell the story of their GDPR compliance:

• Investigate and document the flow of data through your organization. Understand the sources of data the organization has control over, the systems or databases that data is stored in, the controls in place to protect that data, and how and when it's transmitted to third parties.

• Create records of processing and a process going forward for keeping those records up to date.

• Audit vendors and update agreements to include GDPR compliant provisions.

• Track the key requirements of the GDPR and document the data protection policies in place to address those obligations. Create a procedure for data breach response, data retention, and responding to data subject requests.

• Create a DPIA process—including a system to determine when a DPIA is needed and the team in charge of completion.

• Create a schedule and process to periodically audit the effectiveness of your data governance program.

• Conduct annual privacy training for employees.

While the process of preparing for the GDPR may be lengthy and expensive, it may ultimately give information security and internal data governance teams the resources needed to more effectively and strategically manage an organization's data. And, as the GDPR creates affirmative obligations for controllers to vet third party vendors for compliance with the GDPR's obligations, being able to demonstrate compliance with the GDPR through a strong data governance program won't just be a required regulatory obligation; it may be a selling point that distinguishes you as an organization that is safe to do business with.