THE
NATIONAL LAW REVIEW

Article 29 Working Party Issues Guidance on Breach-Notification Obligations under GDPR

Thursday, October 26, 2017

The Article 29 Working Party (WP29) recently issued guidelines regarding data controllers' notification obligations following security breaches involving the personal data of EU citizens.

Under the General Data Protection Regulation (GDPR), data controllers—including U.S.-based companies—are required to notify their lead EU supervisory authority about data breaches involving personal data of EU citizens unless "the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."

Controllers must also notify EU citizens of a data breach if there is a "high risk to the rights and freedoms of natural persons." The WP29's guidelines are intended to help data controllers better understand when notification is required and what processes they should have in place in order to meet their obligations.

Ballard Spahr LLP

Article By Odia Kagan
Philip N. YannellaFred G. DeRitis
Roshni PatelBallard Spahr LLPLegal Alerts

Communications, Media & Internet
Consumer Protection
Corporate & Business Organizations
Global
European Union

One issue of critical importance to U.S. companies is the timing of notifications to European data regulators. The guidelines direct that a data controller must report "where feasible" within 72 hours to its "lead regulatory authority" in such cases where there has been an "accidental or unlawful destruction, loss, alteration, unauthorized disclosures or access to personal data." This 72-hour requirement—much faster than most U.S. laws—is triggered by a company's awareness that a security incident has occurred and personal data has been compromised.

The guidelines do not provide a bright-line rule for awareness. A company gains awareness when it has a "reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised."

The definition of a data compromise under the GDPR is broader than under most U.S. state laws. Under the GDPR, a data compromise can occur where the confidentiality, availability, and integrity of the data is affected. This can be triggered by anything that affects, even temporarily, the availability of data, such as ransomware or a power outage. Similarly, the definition of "personal data" under the GDPR is significantly broader than under U.S. law, and includes any information that can be used, directly or indirectly, to identify an individual, including IP addresses and network passwords.

The WP29 also provided guidance on the scenarios that would not trigger a notification. One important exception is where the breach is "unlikely to result in a risk to the rights and freedoms of natural persons," such as a breach of publicly available data.

Like many state data-breach laws in the United States, the GDPR also provides an exception to reporting for encrypted data (if the keys are not also lost and backups are available). There is, however, no *de minimis* threshold for reporting, as there is under some state laws. Notification may be required even if only a few individuals are affected.

The guidelines identify several operational requirements for companies to comply with breach reporting obligations. First, the GDPR requires documentation of a security incident, even if not reportable. The guidelines encourage companies to create internal "registers" of breaches. This will require legal input to verify that a

security incident meets GDPR definition and should, therefore, be documented. Also, contracts between data controllers and data processors must also explicitly state the processor's obligations to report a data breach to the data controller—a provision that many U.S. controllers do not include in their standard contracts with processors.

Although data controllers must report to their lead regulatory authority within 72 hours, when feasible, the guidance acknowledges that in many instances, controllers may not have complete knowledge of the facts at the time of the initial notification. The WP29 allows for controllers to provide follow-up reports to regulatory authorities and to bundle reporting requirements where multiple breaches occur that involve the same kind of personal data arising in the same fashion.

Notably, reporting to individuals can be done via text, email, letter, or—in certain circumstances—by using public notice mechanisms, such as a rolling banner on a website.

U.S. companies subject to the data breach reporting requirements under the GDPR should revise their incident-response plans to include the need for exigent investigation, determination of need to report, and if necessary, notification to the proper supervisory authority. U.S.-based companies should also include in all contracts with data processors an obligation to notify the company if the processor experiences a breach of personal data. Companies should also identify their lead regulatory authority in the EU, participate in table top exercises in order to test and ensure compliance to GDPR, and consider a process to register all data incidents involving EU personal data, reportable or not.

Source URL: https://www.natlawreview.com/article/article-29-working-party-issues-guidance-breach-notification-obligations-under-gdpr