The Article 29 Working Party Releases Draft Guidelines on Breach Notification

OCTOBER 24, 2017

On October 18, the Article 29 Working Party released its draft of "Guidelines on Personal data breach notification under Regulation 2016/679" ("Guidelines on Personal data breach notification," WP250). The guidelines are not final yet and stakeholders may comment on these guidelines until November 28.

Guidelines on Personal Data Breach Notification

The GDPR introduces pan-European requirements for the notification of personal data breaches. The competent national supervisory authority must be notified unless a breach is unlikely to result in risk to the rights and freedoms of individuals (Art. 33 GDPR). In certain cases, individuals whose personal data has been affected by the breach should be informed (Art. 34 GDPR). The guidelines provide detailed explanations regarding mandatory data breach notification, the "key triggers" for such a notification, related communication requirements and exceptions to the notification obligation.

- **What is a personal data breach?** The GDPR only applies where there is a breach of personal data and, as a result, the controller will be unable to ensure compliance with the processing of personal data as outlined in Article 5 GDPR. This highlights the difference between a security incident and a personal data breach. Essentially, while all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches. It is worth mentioning that the Article 29 Working Party takes the view that a mere temporary loss of availability should be considered to be a security breach, and might require notification, if the non-availability likely affects the rights and freedoms of natural persons—an interpretation that is not obvious from the wording of Article 4(12).
- **When must a controller notify the personal data breach to the competent supervisory authority?** In the case of a personal data breach, the controller must notify the appropriate authority of such breach "not later than 72 hours after becoming aware if it" (Art. 33(1) GDPR). The Article 29 Working Party considers a controller as having become "aware" when that controller believes, with a reasonable degree of certainty, that a security incident, which has led to personal data being compromised, has occurred. This will depend on the

circumstances of the specific breach. After first being informed of a potential breach by an individual, a media organization, or another source, or when it has itself detected a security incident, the controller may undertake a short period of investigation to establish whether a breach has in fact occurred. The controller should therefore have an internal process in place to be able to detect and address such breaches. During this period of investigation, the controller may not be regarded as being "aware." If the data controller cannot notify the supervisory authority within 72 hours, delayed notification may be permitted if reasons for the delay are provided. Here, the Article 29 Working Party is taking the somewhat surprising view that the controller should be considered as "aware" once its processor has become "aware."

- **Which information must the controller provide to the supervisory authority?** Art. 33 (3) GDPR sets the minimum amount of information the controller needs to provide to the supervisory authority. Depending on the nature of the breach, further investigations by the controller may be necessary to establish all the relevant facts relating to the incident. The GDPR recognizes that controllers will not always have all necessary information concerning a breach within 72 hours of becoming aware of it and so it allows for notification in phases.
- **When is a notification to the supervisory authority not required?** Notifications to supervisory authorities do not need to be made for data breaches that are "unlikely to result in a risk to the rights and freedoms of natural persons." (Art. 33 (1) GDPR). For example, if a data breach involved personal data that was already publicly available, further disclosure of such data would not constitute a likely risk. Another example is the theft of securely encrypted data for which the confidentiality of the key remained intact or uncompromised by the breach. Such a breach is unlikely to adversely affect individuals. On the other hand, the Article 29 Working Party stated that if there are no backups of the encrypted personal data, then there is an availability breach, which could pose a risk to individuals.
- **When is the notification of the data subject required and in which cases is it not?** In certain cases, the controller is also required to communicate the breach to the data subjects if the breach "is likely to result in a high risk to the rights and freedoms of natural persons" and the conditions under Art. 34 (3) GDPR, which provide for exceptions to the notification of individuals, are not met. In accordance with the Accountability Principle, the controller should be able to demonstrate to the Supervisory Authority that it meets one or more of these conditions, e.g. appropriate technical and organizational measures to protect personal data, particularly those measures that render such data unintelligible to any person who is not authorized to access it.
- **Which factors should be considered when assessing risk?** As the Article 29 Working Party explains, "risk to the rights and freedoms of individuals" is the "key trigger" for the notification to the supervisory authority, while "high risk to the rights and freedoms of individuals" is the "key trigger" for communication to the data subjects. The Article 29 Working Party therefore recommends that the risk assessment should consider the following criteria: Type of breach; nature, sensitivity, and volume of personal data breached; ease of identification of individuals; severity of consequences for individuals; special characteristics of individuals (e.g., children); number of affected individuals; and special

characteristics of the data controller.

The guidelines also provide useful examples of various types of personal data breaches and who would need to be notified in different scenarios, and a flowchart illustrating the required steps in the course of an assessment.

Authors

Dr. Martin Braun

PARTNER

martin.braun@wilmerhale.com

+49 69 27 10 78 207