Frankfurt Kurnit Klein + Selz PC

Focus on the Data

Unique Insights and Practical Guidance on Privacy and Data Security Issues Worldwide

European Data Protection Board Issues Guidelines on Data Breaches

By Elliott Siebers on February 4, 2021

On January 14, 2021, the European Data Protection Board ("EDPB") adopted **Guidelines 01/2021 on Examples Regarding Data Breach Notification** ("Guidelines"). The Guidelines complement prior guidelines issued by the Article 29 Working Party in October 2017; namely, the **Guidelines on Personal Data Breach Notification under Regulation 2016/679, ("GDPR"), WP 250**. The Guidelines are not yet final, pending a public comment period that concludes on March 7, 2021. While the final version of these Guidelines informed by public comments may vary slightly, they are not likely to change drastically from

the current version as it draws on the experiences of European national supervisory authorities in responding to data breach notifications since the GDPR became effective.

The Guidelines compile case-based examples from the experiences of supervisory authorities with the aim of helping controllers, or organizations that decide how individuals' data gets processed, to better decide how to handle data breaches and what factors to consider in making risk assessments. There are a multitude of cases in the Guidelines, making it a practice-oriented resource for organizations to refer to when implementing or reviewing their own technical and organizational measures. The cases fall into the general categories of ransomware and data exfiltration attacks, as well as "internal" risks posed by employees, lost or stolen devices, social engineering attacks, and third-party relationships. As to each category, various examples are provided, together with an analysis of appropriate prior measures and risk assessment and mitigation and obligations. In most cases, organizational and technical measures for preventing/mitigating the impacts of the particular type of breach in question are also considered. (However, the EDPB notes that if the circumstances of actual incidents differ from the examples provided they may result in different risks, which may require alternative steps to be taken.)

The GDPR defines a personal data breach as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed*." The GDPR also recognizes that the harm individuals may face as a result of a breach can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals. One of the most important obligations of the data controller is to evaluate these risks to the rights and freedoms of data subjects and to implement appropriate technical and organizational measures to address them. Data controllers must consider these risks to individuals' rights and freedoms and implement suitable technical and organizational measures to tackle them.

Under the GDPR, controllers are required to document personal data breaches; notify the competent supervisory authority of breaches (within 72 hours of learning of the breach), unless they are unlikely to result in risks to individuals' rights and freedoms; and inform individuals of breaches if they are likely to lead to high risks to the data subjects' rights and freedoms. In some cases,

the Guidelines note, controllers will be able to appreciate that an incident is likely to result in a risk and will need to be notified. In those cases, notifying is a relatively straightforward decision. However, in other cases "controllers do not need to wait until the risk and impact surrounding the breach have been fully considered, as the full risk assessment can take place in parallel with notification, and information obtained can be made available to supervisory authorities in stages without excessive further delay. It is also important to note that controllers should not wait for a detailed forensic examination and (early) mitigation steps before deciding whether breaches are likely to result in a risk and should therefore be notified – they should make this assessment on discovering the breach." (emphasis added.)

For organizations learning of a breach, but still unsure whether there is a likely risk to the rights or freedoms of individuals, the Guidelines from the EDPB suggest a fairly low threshold as to when to provide notice to a supervisory authority within 72 hours, and that on-going mitigation or forensic investigation steps are not on their own sufficient reasons for a delay in notification.

The Guidelines underscore the fact that all controllers should implement data breach policies and procedures with clear accountability structures. Appropriate personal data breach management training for relevant personnel and accountability is important, as is data protection by design. Personal data breach handbooks are also recommended as roadmaps for how to handle personal data breaches.

Klein + Selz