LATHAM & WATKINS LLP

Global Privacy & Security Compliance Law Blog

Commentary on Global Privacy and Security Issues of Today

5 Ways for Companies to Limit GDPR Penalties

By Latham & Watkins LLP on January 25, 2019

Posted in GDPR, Privacy

EU data protection authorities are imposing increased penalties under the GDPR, with more proceedings forecast for 2019.

By Tim Wybitul, Prof. Dr. Thomas Grützner, Dr. Wolf-Tassilo Böhm, and Dr. Isabelle Brams

The General Data Protection Regulation (GDPR) has been in effect since May 2018. Although the French data protection authority (CNIL) has imposed the highest fine to date — €50 million on 21 January 2019 — German federal data protection authorities have already imposed fines for GDPR infringements in 41 cases nationwide and say that they have "very many" additional fine proceedings in progress. This first wave of fines has come from five German authorities, with 11 authorities having not yet imposed any fines under the GDPR.

Under the former German data protection law, companies faced a maximum penalty of €300,000 for violations. However, the GDPR provides authorities with different disciplinary options and they can now impose fines of up to €20 million or more. The maximum fine may amount to up to 4% of the worldwide annual turnover. Hence, corporates with an annual revenue of more than €500 million may face fines exceeding the €20 million threshold.

What should companies do to prepare for and to defend against GDPR fines?

This checklist outlines five key measures companies can take to prepare for GDPR investigations:

1. **Implement sound GDPR structures**: One of the key aspects of successfully defending against an alleged GDPR violation is to implement a robust data protection management system (DPMS). A DPMS is quite similar to typical compliance management systems and should introduce several lines of defence in order to avoid GDPR violations. The DPMS should include a clear picture of relevant departments' responsibilities, including operational functions, a legal function, an audit function, and often an interna data protection officer. Companies should design their DPMS and underlying documentation processes in a manner which supports potential later investigations effectively.

2. **Identify gaps and vulnerabilities**: Companies should identify business areas or processes that are most likely to cause issues or raise concerns. Often, these areas are either customer-facing or they concern the processing of employees' personal data, and they should be addressed in accordance with identified priorities.
3. **Secure litigation-oriented GDPR documentation**: The GDPR pursues a so-called concept of accountability (Art. 5(2) GDPR) and imposes considerable documentation obligations. Companies shoul structure their GDPR documentation accordingly and be prepared to use this documentation in regulatory proceedings and litigation.
4. **Consider potential claims for immaterial damage compensation**: Art. 82 GDPR gives data subjects the right to sue for compensation for immaterial damages. European courts might use this provision to award compensation for moral damages or emotional suffering. Companies should keep in mind that consumer attorneys may thoroughly monitor the enforcement practice of the general data protection authorities in order to find potential targets for civil litigation. If a company must pay a material GDPR penalty, it becomes easier for the data subject to claim compensation for immaterial damages. Companies must be careful in the communication with data protection authorities and the press to avoid later damage claims.
5. **Assess possible reputational impact of allegations/litigation**: Depending on the nature of a company's business, the mere fact that a data protection authority has initiated investigations may have reputational impact. While data protection authorities have a general confidentiality duty, they are also obliged to make controllers and processors aware of their obligations under GDPR, which may also entai informing the public about pending investigations and sanctions. Consequently, companies should coordinate closely with data protection authorities on public communication.

Key takeaways for companies preparing for GDPR investigations

Companies should have a clear picture of the individual risks and potential penalties that GDPR investigations pose and be adequately prepared to defend regulatory investigations. Companies must determine responsibilities in advance of any investigation, and decision-makers should have a clear action plan to address regulatory requests from data protection authorities, complaints from data subject, or whistleblowers reporting possible shortcomings in GDPR compliance. While most authorities have so far imposed relatively low fines in more straightforward cases most legally complex or contentious cases will take much longer. Finally, the €50 million fine imposed by the GDPR may be the first of many controversial data privacy litigations.