10 Things a General Counsel Must Know About EU Cyber Incidents

LATHAM & WATKINS LLP

1.
YOU Need to Act

Cybersecurity incident response involves multifaceted technical and legal issues. You and your legal team should identify potential pitfalls, plan ahead, and practice your response.

2.
Massive **LEGAL** Exposure

If a cybersecurity incident affects individuals or entities in the EU or the UK, you should avoid exposure under the EU General Data Protection Regulation (GDPR) or similar UK legislation. These risks include fines, damage claims, reputational harm, and other threats to your organization. Breaches or other cybersecurity incidents that are caused or facilitated by process or systems failings might lead to broader investigations by data protection authorities or other regulators into the organization's overall compliance. Companies doing business in Europe now face a new litigation landscape under the EU Directive on Representative Actions. It came into force in June 2023 and will also cover GDPR damages claims. The Directive brings increased opportunities for consumers to enforce their rights. Cross-border collective actions within the EU will be easier to bring and more complex to defend.

3.
72-Hour Reporting Deadline

Act quickly. When a company learns of an actual or possible cybersecurity incident with EU relevance, it must notify its competent data protection authority, unless the incident is unlikely to result in risks to the affected data subjects. Even when not in a crisis and under time pressure, that risk assessment can be challenging. Non-compliance with the reporting obligation can result in high GDPR fines, but notifying unnecessarily can result in unwelcome regulatory intervention at a time when you ought to be focused on responding to the legal aspects of the incident. Even a loss of availability of personal data (e.g. in the course of a ransomware attack) can trigger GDPR reporting obligations, too. To make matters more complex, national laws may provide for additional and more specific reporting obligations and deadlines that apply simultaneously to GDPR notification requirements.

4.
Data Subject and other Comms

If a cybersecurity incident or other personal data breach will likely put natural persons' rights and freedoms at high risk, the affected company must inform the concerned data subjects without undue delay. Even if there is no obligation to report, an affected organisation can expect questions from customers and other business partners impacted by the outage, curious employees, and even the media. Thus, a coordinated and effective communication strategy is crucial to avoid negative press and related business risks.

5.
High GDPR Fines

GDPR violations, including of any of the obligations described in this overview, can result in multimillion-euro fines. The maximum penalty per infringement is €20 million or 4 percent of the affected company's revenue, whichever is greater. The highest fine that EU data protection authorities have imposed to date exceeded €700 million. The EU authorities recently adopted a GDPR fine calculation model that increases risks for large companies or groups. In many cases, this calculation model will exhaust the fine range quite extensively.

6.
GDPR Damage Claims

The GDPR allows data subjects to claim immaterial damages for the disclosure or loss of their personal data. Because cybersecurity incidents usually affect many data subjects, your company can easily face multimillion-euro follow-on damages claims from a class of affected individuals. In such (mass) proceedings, plaintiffs often argue that the defendant violated the GDPR and/or other legal requirements by providing insufficient cybersecurity and, hence, data security. Consequently, they claim immaterial damages compensation for the disclosure of their data in the course of the cybersecurity incident.

7.
Think Globally

Cybersecurity incidents rarely respect jurisdictional borders. Notification obligations, liability, and other consequences often expand beyond EU/UK or US laws, for instance. Dealing with such scenarios often requires a global response and involving local counsel. Identifying experts in key geographies in advance can save crucial time in a crisis.

8.
Preparation Is Key

The GDPR requires entities to implement comprehensive security measures, including anonymization, pseudonymization, and encryption. Equally important, you should review your company's cybersecurity incident response plan (CIRP).You can ensure that the legal considerations described here are integrated into the CIRP and allow you to react quickly and methodically in an emergency. Failure to implement adequate technical and organizational measures poses significant risk to data and systems and exposes organizations to the risk of steep fines and mass damage claims.

9.
Awareness and Training

To comply with GDPR obligations, implement mandatory privacy and cybersecurity trainings with regular 'refreshers' to ensure that your company's employees know how to detect and avoid potential cyber incidents and resulting risks. Such trainings and other security and privacy measures need to be documented in accordance with GDPR requirements.

10.
When in Doubt Call us.

Call us for immediate GDPR and global cybersecurity incident advice. We can also help you devise a plan for potential future threats, including a CIRP, running crisis simulations (tabletop exercises) and establishing contacts with local counsel and other experts. See our contacts below.

Please also click here to visit our Privacy & Cyber presence

Your Team

Myria Saarinen
Partner, Paris
T +33.1.40.62.28.43
E myria.saarinen@lw.com

James Lloyd
Partner, London
T +44.20.7866.2668
E james.lloyd@lw.com

Michael H. Rubin
Partner, San Francisco, Silicon Valley
T +1.415.395.8154
E michael.rubin@lw.com

Kieran Donovan
Partner, Hong Kong
T +852.2912.2701
E kieran.donovan@lw.com

Antony (Tony) Kim
Partner, Washington, D.C.
T +1.202.637.3394
E antony.kim@lw.com

Tim Wybitul
Partner, Frankfurt
T +49.69.6062.6560
E tim.wybitul@lw.com

Wolf-Tassilo Böhm
Counsel, Frankfurt
T +49.69.6062.6558
E wolf.boehm@lw.com

José María Alonso
Partner, Madrid
T +34.91.791.5113
E jose.alonso@lw.com

Gail E. Crawford
Partner, London
T +44.20.7710.3001
E gail.crawford@lw.com

Jennifer C. Archie
Partner, Washington, D.C.
T +1.202.637.2205
E jennifer.archie@lw.com

Serrin Turner
Partner, New York
T +1.212.906.1330
E serrin.turner@lw.com

Latham & Watkins operates worldwide as a limited liability partnership organized under the laws of the State of Delaware (USA) with affiliated limited liability partnerships conducting the practice in France, Hong Kong, Italy, Singapore, and the United Kingdom and as an affiliated partnership conducting the practice in Japan. Latham & Watkins operates in Israel through a limited liability company. Latham & Watkins operates in South Korea as a Foreign Legal Consultant Office. Latham & Watkins works in cooperation with the Law Firm of Salman M. Al-Sudairi in the Kingdom of Saudi Arabia. © Copyright 2022 Latham & Watkins. All Rights Reserved.