Netherlands Imposes Record-Breaking Data Privacy Fine on Uber: 4 Key Steps Companies Can Take to Ensure Compliance

Insights
10.03.24

Dutch data privacy officials recently imposed a staggering penalty on Uber – €290 million ($324 million) – for allegedly breaching the European Union's comprehensive data privacy and security law. This groundbreaking fine is yet further proof that data privacy is a high-stakes battleground for businesses around the globe. And as the decision makes clear, understanding and navigating data privacy laws in every jurisdiction in which you operate has become more important than ever. Here's what you need to know about this development and four steps employers can take to manage their risk.

DPA Fines Uber €290 Million

According to the Dutch Data Protection Authority (DPA), Uber allegedly collected a range of private information from European drivers, including account information, location data, payment information, and in some cases, criminal and health-related histories of their drivers.

Over the span of two years, officials allege that Uber transferred this information to servers based in San Francisco, California. The DPA concluded that Uber had not sufficiently protected this data during the transfer, amounting to a "very serious violation" of the General Data Protection Regulation (GDPR). Although Uber has appealed the fine, this case highlights the serious consequences of non-compliance as data privacy laws continue to evolve.

Understanding the GDPR and Global Data Privacy Landscape

Enacted in 2018, the GDPR is considered one of the most rigorous data privacy laws in the world. It has strict conditions on the processing or collection of personal data, including information related to individuals' racial or ethnic origin, political opinions, religious beliefs, or health information.

GDPR's foundational principal is recognizing the rights of individuals whose data is processed (e.g., customers or website visitors), including the right to be informed about the use of their data, the right to confirm whether an organization has obtained their data, and the right to rectify or delete the data collected.

GDPR's scope extends beyond the EU, applying to any entity that offers goods or services to, or processes the personal data of, EU residents and citizens. Compliance is enforced through a two-

tier penalty system, with fines reaching up to €20 million or 4% of global revenue.

And the EU is not alone. For example, in 2021, China enacted the Personal Information Protection Law (PIPL) and Data Security Law (DSL) which strengthened existing data privacy laws (read more about these laws here and here). Like the GDPR, China's PIPL expands its regulatory scope to companies ("data processors") outside China if they offer products, services, or conduct data analysis on persons within China. China's DSL also governs data processing outside its borders, imposing more stringent obligations on entities and individuals regarding data classification, risk controls and assessments, and cross-border transfers. Other countries have also introduced comprehensive data privacy laws, including Mexico, Australia, Canada, Japan, South Korea, and Brazil.

An increasing number of U.S. states have taken similar action. In 2023, by voter referendum, California passed the California Privacy Rights Act (CPRA), which builds upon the data privacy requirements that were established in 2018 by the California Consumer Protection Act (CCPA) by increasing employers' responsibilities in the collection, storage, use, and sharing of employee personal data. As of the date of this publication, 19 states have passed some form of data privacy law and that number will no doubt increase in the coming years.

How Can Employers Manage Data Privacy Compliance?

It is essential for businesses to be informed about specific privacy regulations in the jurisdictions where they operate. With more jurisdictions enacting strict data privacy laws (many of which overlap or sometimes contradict others), compliance is more challenging than ever, but four key steps can help simplify the process.

1. *Identify Where Your Business Operates*

A critical first step is identifying all the jurisdictions in which your business operates to determine applicable privacy laws. This inquiry is not limited to areas where employees are located; it can also include jurisdictions where your business has customers. For instance, serving EU customers may require adherence to GDPR, even if your business is based elsewhere. Understanding your business' footprint will help tailor the data privacy strategy to meet specific legal requirements.

2. *Invest in Robust Data Protection Programs*

Implement robust data protection measures, which may vary by jurisdiction. These can include encryption methodologies, secure access controls, and data minimization to limit unnecessary data collection.

3. *Audit Your Systems*

Regular audits of data handling, storage, and transfer practices are also essential. Audits help identify risks and non-compliance, allowing you to address vulnerabilities before they lead to costly breaches or violations.

4. *Stay Informed about Legal Developments*

Stay up-to-date with data privacy laws and regulations, both locally and globally. As data privacy rapidly evolves, ongoing diligence is crucial for compliance. Engage with legal and privacy experts to assess how new regulations may affect your business. Partnering with Fisher Phillips can help shape your compliance strategy and offer advice tailored to your specific needs.

Conclusion

We will continue to monitor developments related to data privacy laws and regulations across the world. Make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information. If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our International Practice Group or Privacy and Cyber Group.

Related People

Nazanin Afshar
Partner
818.230.4259
Email

Chelsea Viola
Associate
213.403.9626
Email

Service Focus

Privacy and Cyber

International