Uber Fined over $1.1Million by EU Data Protection Authorities: Six Lessons Learned

December 17, 2018

What happened?

On November 27, 2018, Uber was hit with fines from the UK and Dutch data protection authorities totalling nearly $1.2 million in connection with the 2016 data breach that affected more than 57 million Uber customers and drivers.

Debevoise & Plimpton

Why was Uber fined?

The UK Information Commissioner's Office ("ICO") fined Uber £385,000 (approx. $485,000) for failing to take appropriate technical and organisational measures to safeguard individuals' personal data, while the Dutch Data Protection Authority ("Dutch DPA") fined Uber €600,000 (approx. $678,000) for failing to report the breach within 72 hours. The fines come on the heels of a $148 million settlement in the United States relating to the same incident.

Both fines were issued under UK and Dutch laws predating the EU General Data Protection Regulation ("GDPR") because the breach occurred before the GDPR came into force. They nevertheless offer useful insight into data protection authorities' evolving expectations.

What are the lessons learned?

- Two-factor authentication may soon become a *de facto* requirement. In finding that Uber's security arrangements were inadequate, the ICO appears to have expected Uber to have implemented two-factor authentication for access to the GitHub software development platform, which was breached.

- Good password hygiene goes beyond forced password changes. The ICO called out Uber's failure to expressly prohibit employees from re-using credentials for third-party platforms used in work activities. This suggests an expectation that companies require their employees to use different passwords for each work-related activity and that those passwords be different from personal passwords.

- Beware plain-text credential storage. The account credential that led to the breach was stored as plain text in a piece of code, a vulnerability that the ICO suggested

contributed to its decision to levy a fine. Companies should carefully monitor and assess where and how credentials are stored and transmitted, along with the associated cybersecurity implications.

- Don't use bug bounty programmes to hide data breaches. Uber opted to treat the breach and the $100,000 demand that Uber paid for the data to be destroyed as a bug bounty even though it fell outside the scope of Uber's official bug bounty programme. Companies should ensure that they accurately identify personal data breaches so they can be dealt with appropriately under the GDPR.

- Quick and efficient cross-border coordination is crucial. While the ICO fine was limited to Uber's European entities, the Dutch DPA held Uber's Dutch entity and its ultimate U.S. parent company jointly liable for failing to meet the Dutch (and now the GDPR's) 72-hour breach notification requirement. The Dutch DPA's decision indicates that they considered the clock on breach notification to have started running in November 2016, when the U.S. parent company became aware of the breach—even though the Dutch entity was not informed of it until almost a year later.

- Be prepared to engage with multiple data protection authorities simultaneously. The ICO and the Dutch DPA strategically split enforcement to produce maximum impact. The ICO penalised Uber for security failings while the Dutch DPA fined Uber for not reporting the breach within 72 hours, which was not a requirement in the UK at the time. Although the GDPR's Lead Supervisory Authority concept might mitigate the risk of multiple EU DPAs piling on cross-border incidents, the Uber fine may serve as a model of multinational enforcement actions in the future.

Debevoise advises EU and non-EU businesses on all areas of GDPR compliance, including incident response and interaction with data protection authorities. We look forward to discussing with you the issues raised by these fines.

Jane Shvets
Partner, London
+44 20 7786 9163
jshvets@debevoise.com

Robert Maddox
Associate, London
+44 20 7786 5407
rmaddox@debevoise.com