The Computer & Internet Lawyer

Volume 42 ▲ Number 1 ▲ January 2025

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Dutch Data Protection Authority Fines Uber €290 Million for GDPR Data Transfer Violation

By Daniel K. Alvarez, Laura E. Jehl, Briony Pollard, Susan Rohol and Kari Prochaska

On August 26, 2024, the Dutch Data Protection Authority (Dutch DPA) published its decision to fine Uber Technologies, Inc. and Uber B.V. (Uber) €290 million for a violation of the General Data Protection Regulation (GDPR). Specifically, the Dutch DPA found that, for a 27-month period, Uber failed to implement appropriate safeguards required under the GDPR for transferring EEA-based drivers' personal data to the United States (Decision). While it is anticipated that Uber will appeal the ruling, the Decision is noteworthy both for exacerbating the uncertainty in the international data transfer landscape, particularly for U.S.-based companies that transfer employee data from the EEA to the United States, as well as for the magnitude of the fine and what it tells other companies about the potential price of being wrong.

The authors, attorneys with Willkie Farr & Gallagher LLP, may be contacted at dalvarez@willkie.com, ljehl@willkie.com, bpollard@willkie.com, srohol@willkie.com and kprochaska@willkie.com, respectively.

BACKGROUND

The Dutch DPA's investigation into Uber originated with complaints by drivers to the French data protection authority regarding the company's transfers of driver personal data (including special category and criminal record data) from the EEA to the United States, the latter being where Uber's centralized IT infrastructure is located. Since Uber's European headquarters are based in the Netherlands, the matter was transferred to the Dutch DPA for adjudication.

During the period between the invalidation of the EU-U.S. Privacy Shield by the Court of Justice of the European Union (CJEU) and Uber's self-certification under the EU-U.S. Data Privacy Framework, Uber removed the Standard Contractual Clauses (SCCs) from its data sharing agreements between its EEA and U.S. entities, relying on guidance in the European Commission Q&A on the 2021 EU model contractual clauses (EU Q&A) indicating that the controller-to-controller SCCs would not be appropriate in circumstances where the importing entity's processing operations are already directly subject to the GDPR

under Article 3. As described below, the Dutch DPA rejected this position as inconsistent with the requirements of the GDPR.

The DPA stated that it has coordinated its decision with other EU data protection authorities, so it is possible that other data protection authorities may reach a similar determination to that of the Dutch DPA regarding personal data transfers. It is expected that Uber will appeal the Decision, so the door is not shut on these issues.

KEY TAKEAWAYS

Adequate Safeguards Must Be Implemented for International Intra-Group Personal Data Transfers

Uber argued that both Uber's U.S. entity and its EEA entity were subject to the GDPR under Article 3 as joint controllers, so further compliance with the requirements of Chapter V of the GDPR was not required. The Dutch DPA disagreed and stated (among other things) that because it is difficult to enforce compliance with the GDPR against foreign companies, the data transfer requirements described in Chapter V of the GDPR place a direct obligation on parties that process personal data in third countries. Accordingly, the parties must comply with all obligations under the GDPR, including those that require appropriate safeguards for such data transfer.

Further, Uber argued that when a driver provides their personal data to Uber, there is no "onward transfer" from Uber EEA to Uber U.S. Rejecting this argument, the Dutch DPA determined that there *is* an "onward transfer" from Uber EEA (i.e., the data exporter) of the driver's personal data to Uber U.S., as data importer. Noting that drivers enter personal data on the Uber platform through the driver's personal device, the Dutch DPA reasoned that such personal data ends up on Uber's systems through an arrangement between Uber EEA – not Uber U.S. – and the drivers. Accordingly, the Dutch DPA concluded that a personal data transfer from the EEA to the United States had occurred and held that a level of data protection for that personal data transfer must be guaranteed under the GDPR.

Derogations Under Article 49 of the GDPR Are Limited

Uber argued that if a transfer of personal data occurred, such transfer was lawful in accordance with a derogation in Article 49 of the GDPR, because the transfer was necessary for the performance of a contract between Uber and the driver.

The Dutch DPA rejected Uber's argument that the particular transfer was "incidental," because such transfers could not be characterized as non-repetitive or as taking place at irregular intervals. Rather, the Dutch DPA determined that transfers between Uber's EEA and U.S. entities were systematic, repetitive, and ongoing, as part of a stable and ongoing business relationship. Further, the Dutch DPA concluded the existence of a contract does not in itself constitute "necessity"; in order for a transfer to be "necessary" there should not be practicable, less intrusive alternatives available to the data controller. The Dutch DPA was not convinced by Uber's argument that centralized data processing in the United States is crucial to Uber's ability to provide services and speculated that Uber was motivated by efficiency reasons, which was not enough to satisfy the "necessity" requirement.

Proportionality of the Fine Assessed By the Seriousness of the Violation

While some commentators have posited that the level of the fine seems excessive, the Dutch DPA outlined its rationale for the fine in the Decision. In particular, the Dutch DPA focused on the European Data Protection Board guidelines indicating that the level of severity of the violation should be proportional to the amount of the fine. As the Dutch DPA determined Uber's violation to be serious, it evaluated the fine under the parameters of the maximum level available under Article 44, the higher of €20 million or 4% annual turnover.

In evaluating the severity of the violation, the Dutch DPA considered the particularly sensitive nature of the drivers' personal data (e.g., criminal personal data) and regarded the period during which the violation existed (i.e., 27 months), as significant. The Dutch DPA did not regard the fine as disproportionate since it was below the statutory maximum that could have been imposed on Uber.

Under Article 83 of the GDPR, data protection authorities have the power to level fines for intentional or negligent conduct. The Dutch DPA noted that a data controller commits a violation, intentionally or negligently, if they could have not been unaware that the conduct constituted a violation, regardless of whether they were aware that they were violating the GDPR. The Dutch DPA determined that Uber "could have known" based on the GDPR, CJEU case law, and the decisions of other data protection regulators, that it was foreseeable that a transfer of personal data to the United States from the EEA would require additional safeguards.

WHAT'S NEXT?

The biggest takeaway is the additional uncertainty this decision adds to an already cloudy international data transfer landscape. In particular, the Decision casts doubt on whether companies can rely on European Commission guidance contained in Q&As – either for compliance purposes or to help mitigate potential penalties for non-compliance if a data protection authority disagrees with the company's approach.