WERKSMANS
ATTORNEYS

REGULATORY

How you driven through to how safe your personal information is with Uber

17 October 2024 *4 min read*

> *"Uber did not meet the requirements of the GDPR to ensure the level of protection to the data with regard to transfers to the US. That is very serious."*
>
> *(Aleid Wolfsen, Chairman of the Dutch Data Protection Authority)*

Uber – the giant ride-hailing platform – has been fined 290 million euros (approximately 5.5 billion rand) for allegedly transferring personal data[1] from European Union ("**EU**") to United States ("**US**") based servers without adequate protections in place.

From a South African perspective, lessons from Uber's case resonate given that the Protection of Personal Information 4 of 2013 ("**POPIA**") mirrors the principles of the General Data Protection Regulation 2016/679 ("**GDPR**"). Much like the GDPR's standards, POPIA requires companies to ensure that when personal data is transferred outside South Africa's borders, the recipient must be bound by adequate levels of protection or substantially similar safeguards as set out in POPIA.[2]

As South African businesses continue to grow and integrate with global markets, Uber's case serves as a reminder that whether in Amsterdam or Johannesburg, data protection laws are watching and the consequences of non-compliance are severe.

The Dutch Data Protection Authority ("**DPA**") found that –[3]

- Uber processed, among others, sensitive information of drivers from Europe and retained it on servers in the US. This included information relating to account details and taxi licences, location data, photos, payment details, identity documents, and in some cases even criminal and medical data of drivers;
- for a period of over two (2) years, Uber transferred the above personal data to Uber's headquarters in the US without using transfer tools as required by the GDPR;
- as Uber no longer used standard contractual clauses from August 2021, the personal data of drivers from the EU were insufficiently protected and Uber's reliance on the Privacy Shield was insufficient; and
- standard contractual clauses could still provide a valid basis for transferring data to countries outside the EU, but only if an equivalent level of protection can be guaranteed in practice.

As reported, an Uber statement read –[4]

> *"This flawed decision and extraordinary fine are completely unjustified. Uber's cross-border data transfer process was compliant with GDPR during a three-year period of immense uncertainty between the EU and US. We will appeal and remain confident that common sense will prevail."*

The decision of the DPA highlights the ongoing challenges of cross-border data transfers post-GDPR, especially following the invalidation of the EU-US Privacy Shield.[5] However, as found by the DPA, as Uber stopped using standard contractual clauses in August 2021, the DPA

found that the data of EU drivers was insufficiently protected.

With the EU's GDPR and South Africa's POPIA both emphasising the need for robust safeguards when personal data crosses national borders, South African businesses must consequently take note and be vigilant in ensuring compliance. This is particularly prudent in today's world where the digital economy continues to expand and global data flows are common and more important to business operations. South African businesses cannot afford to overlook legal obligations imposed by POPIA. Non-compliance in this regard presents risk of fines, reputational damage and customer mistrust.

Uber's costly lesson is one that should prompt South African businesses to ensure compliance.

If your business deals with international data transfers or requires guidance with POPIA and/or other global data protection laws (such as GDPR), and you have questions, feel free to contact us to explore compliance with data protection laws.

---

[1] Note: The GDPR makes use of the term "personal data". POPIA, on the other hand, makes use of the term "personal information". Both have the same meaning, but the POPIA definition extends to juristic persons. To avoid prolixity, this article makes use of the word "personal data".

[2] In addition, there are other grounds upon which a responsible party can rely upon as set out in section 72 of POPIA.

[3] Please see the website of the DPA at https://autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-of-290-million-euro-on-uber-because-of-transfers-of-drivers-data-to-the-us, accessed on 14 October 2024.

[4] See https://apnews.com/article/netherlands-uber-fine-drivers-6fcade85cf70b448babc841f12dd9047, accessed on 14 October 2024.

[5] To this end, in 2020, the European Court of Justice invalidated the EU-US Privacy Shield in a case commonly referred to as "Schrems II". See https://www.upguard.com/blog/eu-us-privacy-shield#:~:text=In%202020%2C%20the%20European%20Court,to%20the%20Safe%20Harbor%20agreement)., accessed on 14 October 2024.

Ahmore Burger-Smidt

Head of Regulatory

View Profile

Dale Adams