Data Privacy and Cybersecurity

Transfers of Personal Data – No Monkey Business Allowed

By: Kelly Hagedorn and Matthew Worby

The German state-level data protection authority for Bavaria (BDPA) recently issued a decision stating that the transfer of personal data to the US-based email marketing platform Mailchimp, by a company (which has not been officially named), was unlawful.

Ultimately, the BDPA declined to take formal enforcement action because the company stopped using Mailchimp in response to the complaint. Despite the lack of formal enforcement action, this decision by the BDPA is an important development highlighting the continuing repercussions of the Court of Justice of the EU's (CJEU) ruling in *Schrems II* for international data transfers out of the European Union.[1] For detail about *Schrems II* please see our client alert, available here.

The Use of Mailchimp

According to the BDPA decision, the company reportedly transferred personal data to Mailchimp, a US entity. The transfer was undertaken on the basis of EU standard contractual clauses (SCCs), an ordinary measure taken to ensure the protection of personal data when that personal data is transferred out of the EU; and one that the CJEU upheld in *Schrems II*.

The BDPA, however, decided that, despite the use of SCCs, the company had failed to assess if additional measures were required to protect the personal data in accordance with *Schrems II*.

The BDPA took this view because it considered the personal data in question to be at risk of access by the US government. The BDPA determined that Mailchimp may meet the definition of an "electronic communication service provider" under the US Foreign Intelligence Surveillance Act, meaning that Mailchimp might be required to disclose personal data if requested by the US government.[2] The protections afforded to the personal data by the General Data Protection Regulation (GDPR) could not therefore be assured when the personal data reached the United States. This kind of interpretation of *Schrems II* is precisely the outcome that many multi-national companies feared when *Schrems II* upheld the use of SCCs, but cast doubt on the effectiveness of SCCs as a mechanism for transferring of data to the United States.

Practical Steps

It is important to note that neither *Schrems II*, nor the BDPA decision, renders international personal data transfers outside of the European Union and to the United States unlawful. Additional measures can be implemented to ensure the protection of any personal data transferred which could be subject to government access. It was the company's failure to assess the need for additional measures that resulted in the BDPA's decision that the transfers of personal data to Mailchimp were contrary to the GDPR.

The BDPA's decision reinforces the need for entities subject to the GDPR to consider their international data transfers carefully. In particular:

- Companies using data processors outside of the EU should consider the location of the data processors and the applicable laws in those jurisdictions in order to ascertain if personal data transferred could be susceptible to access by government entities; and
- If so, consider which additional protective measures are needed, and implement such measures as necessary. This decision should be clearly documented to ensure appropriate demonstrable

accountability to data protection authorities.

Helpfully, the European Data Protection Board (EDPB) has issued guidance about how to approach this review and mitigation process for international personal transfers outside of the EU. For further information about the EDPB guidance, and what constitutes additional measures, please see our client alert available here. The UK Information Commissioner's Office has stated it will issue its own guidance covering international personal data transfers outside of the UK in due course.

Until the European Union and the United States agree to a new certification program for the trans-Atlantic transfer of data, it is important that businesses in the EU and the US take the analytical steps recommended by the EDPB so as to ensure that their continued use of SCCs remain valid.

---

[1] Case C-311/18, available here.

[2] Foreign Intelligence Surveillance Act section 702 (50 U.S.C. § 1881).

Contact Us

Kelly Hagedorn

khagedorn@jenner.com | Download V-Card

Matthew Worby

mworby@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower

Chair

dbitkower@jenner.com

Download V-Card

David P. Saunders

Co-chair

dsaunders@jenner.com

Download V-Card