BARNES & THORNBURG LLP

ALERTS

Data Privacy Standard Contractual Clauses Called Into Question After Meta Ireland Fine

June 9, 2023

Highlights

Meta Ireland decision by the Ireland Data Protection Authority calls the data protection standard contractual clauses into question

All businesses subject to U.S. Foreign Intelligence Surveillance Act Section 702 and engaging in cross-border transfers could be at risk of violating European Union law

There is currently no clear path forward for cross-border transfers of EU data to the U.S.

On May 22, 2023, the Ireland Data Protection Commission (DPC) fined Meta Ireland 1.2 billion euros for violation of the European Union's General Data Protection Regulation (GDPR). The decision, which levies the largest fine for GDPR violations to date, held Meta Ireland did not adequately protect EU personal data during cross-border data transfers.

Meta, like a majority of businesses, relied upon the GDPR-approved standard contractual clauses (SCCs) and additional safeguards recommended by the *Schrems II* case to provide the legal basis for international data transfers. The DPC held Meta was nevertheless in

RELATED PEOPLE

Brian J. McGinnis
Partner
Indianapolis

P 317-231-6437
F 317-231-7433
brian.mcginnis@btlaw.com

Maddie San Jose
Associate
Indianapolis

P 317-231-6416
F 317-231-7433
msanjose@btlaw.com

RELATED PRACTICE AREAS

Data Security and Privacy
Intellectual Property
International IP

violation due largely to its subjection to U.S. surveillance laws, including the U.S. Foreign Intelligence Surveillance Act (FISA) Section 702 PRISM program.

The DPC expressed that such surveillance laws allow the U.S. government to access personal data of EU citizens even where additional safeguards are in place.

Although this decision deals a particularly large blow to Meta, all entities relying upon SCCs to complete data transfers from the EU to the U.S. are now affected. Due to the continued and wide-reaching effects of the U.S.'s strategy on surveillance, we've now entered yet another period of uncertainty, and the ability to lawfully transfer personal data into the U.S. from the EU and United Kingdom is again in question.

The Meta Decision

The decision from the DPC stated that transfers of data from the EU to the U.S. were "made in circumstances which fail to guarantee a level of protection to data subjects" that is equivalent to protections set out in the GDPR. As a remedy, the DPC has given Meta five months to suspend all transfers of personal data to the U.S., bring its processing activities into compliance with EU law, and delete any EU personal data that been transferred unlawfully under this decision.

The EU has long struggled with how to regulate EU personal data transfers to the U.S. After the invalidation of the U.S.-EU Safe Harbor Agreement and the U.S.-EU Privacy Shield in the *Schrems I & Schrems II* decisions, entities including Meta have mostly relied on SCCs to lawfully transfer EU personal data into the U.S. where U.S. laws are considered to provide substantially less protection.

U.S. Law Impacting EU-U.S. Data Transfers

FISA was originally enacted to authorize and regulate certain governmental electronic communications surveillance for foreign intelligence purposes in 1978, and has been amended most recently in 2015. When Congress enacted the FISA Amendments Act of 2008, it "established a new and independent source of intelligence collection authority, beyond that granted in traditional FISA." One of these additions was Section 702.

Section 702 was added to FISA for the purpose of authorizing the acquisition of foreign intelligence information about non-U.S. individuals. Section 702 barely restricts the U.S.'s ability to surveille foreign data subjects. The DPC decision held that, due to legislation such as Section 702, the EU cannot guarantee that EU personal data transferred to the U.S. will not be accessed by U.S. authorities under such surveillance laws. As this means EU data subjects cannot be afforded the same protections as they are granted under GDPR, the courts have held the U.S.'s system insufficient to protect EU individuals' data.

Due to the far-reaching scope of Section 702, businesses and entities of all kinds could be subject to U.S. orders mandating access to user data for foreign intelligence purposes.

EU-U.S. Privacy Framework

Despite the challenges associated with the Meta decision, a new cross-border data transfer mechanism between the EU and U.S., the EU-U.S Privacy Framework, is in the works. In support of the framework, President Joe Biden signed an Executive Order on Oct. 7, 2022, which implemented safeguards for U.S. intelligence activities, mandated personal information handling requirements, required the U.S. Intelligence Community to update its policies, and noted other mechanisms to promote the secure transfer of data.

The goal of the new transfer mechanism will be to provide a legally secure way for companies to engage in cross-border transfers. While originally intended to replace the Privacy Shield, the framework takes on a new significance and urgency in light of the Meta fine.

Despite the framework's importance, in line with the *Schrems* decisions that invalidated previous adequacy decisions between the EU and U.S., it is anticipated the framework is already facing challenges from the European Parliament, and will almost certainly be challenged once finalized as well. It is unclear when the framework will be passed and go into effect. On May 11, 2023, the European Parliament adopted a resolution that encourages further negotiations regarding effective cross-border transfer mechanisms due to noncompliance with EU laws.

Implications and Next Steps

This Meta decision not only calls into question the validity of SCCs, but also complicates current and future international data transfers between the EU and U.S. Entities relying on SCCs to transfer personal data from the EU to the U.S. will now need to take additional steps to ensure compliance with EU law. To protect themselves, entities should consider:

- Evaluating their personal data transfer policies
- Assessing survey vendor and partner agreements that rely on SCCs or valid transfers
- Determining additional safeguards that can be established to protect or limit any personal data involved in cross-border transfers
- Ensuring they are using the correct form of SCCs in current data transfer mechanisms and only transferring personal data from the EU to the U.S. if absolutely necessary
- Implementing additional safeguards to ensure maximum compliance and to avoid enforcement actions similar to the Meta fine until a new privacy framework is passed

For more information, please contact the Barnes & Thornburg attorney with whom you work or Brian McGinnis at 317-231-6437 or brian.mcginnis@btlaw.com or Maddie San Jose at 317-231-6416 or msanjose@btlaw.com. This alert was drafted with the assistance of Lyric Dawn Menges, summer associate.