Alert

May 30, 2023

COZEN O'CONNOR

Irish Data Protection Commission's Decision Throws Use of Standard Contractual Clauses Into Doubt

On May 22, Ireland's Data Protection Commission (DPC) announced that it had imposed a €1.2 billion fine on Meta Platforms for violating the European Union's General Data Protection Regulation (GDPR) in its use of standard contractual clauses as a mechanism to transfer the personal data of Facebook users from the European Economic Area to the United States. The DPC is also requiring Meta to suspend the transfers. (Previously, on April 13, the European Data Protection Board (EDPB), a consortium of EU member state data protection regulators, had directed the DPC to amend its initial draft decision, which was more sympathetic to Meta.) Meta is appealing these decisions.

This determination is extremely significant, not only for the size of the fine (the largest yet imposed under the GDPR) but also because the European Commission's standard contractual clauses have been the primary legal mechanism for EU-U.S. transfers since the EU's Court of Justice invalidated the EU-U.S. Privacy Shield in 2020 in its landmark *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems* (*Schrems II*) ruling. The court's central concern in that ruling was the same as the Irish DPC's now, namely that the U.S. government's mass surveillance of communications through U.S.-based cloud services, combined with an inability of European residents to seek recourse from an independent tribunal, blocked them from having essentially equivalent privacy protections to those recognized under European law. While the *Schrems II* court held that private companies could still use standard contractual clauses to transfer personal data out of the EU, it also required them to perform, for each data transfer, an assessment of the privacy laws and the actions of government intelligence and law enforcement agencies in the importing country and use supplemental measures (such as encryption) as needed to ensure that EU residents whose data is transferred will have an essentially equivalent level of privacy protection.

Meta made a serious attempt to implement the ruling of the *Schrems II* court as well as guidance from the European Commission and European data protection authorities, bolstering its reliance on the standard contractual clauses with various supplemental measures to protect transferred European data from being accessed by U.S. government agencies. In finding that these measures were insufficient and, therefore, Meta could not use the standard contractual clauses, the Irish DPC underlined a quandary that companies engaging in transatlantic data transfers have been struggling with since 2020: since private companies cannot control the activities of federal agencies and have only limited input in writing the country's laws, can there ever be certainty that data transfers to the U.S. are permitted under GDPR? The actions of the Irish DPC and certain other European data protection authorities seem to refute this and read a *de facto* data localization requirement into GDPR, at least for large cloud services companies like Meta that have been the focus of U.S. intelligence gathering in the past.

All sides now agree that the only solution is a political one. In 2022 the Biden administration and the European Commission negotiated a new EU-U.S. Data Privacy Framework (DPF) to replace the defunct Privacy Shield. The DPF, already partially implemented by executive order, attempts to address the concerns raised in *Schrems II* by imposing limitations on some U.S. signals intelligence gathering and retention and calling for the establishment of an independent Data Protection Review Court, composed of judges not otherwise employed by the U.S. government, to hear appeals from European residents. Companies that self-certify to compliance with the DPF would have the benefit of an adequacy decision from the European Commission, avoiding the need for standard contractual clauses or another legal data transfer mechanism. Although the European Commission circulated a draft adequacy decision in December 2022, it has not yet adopted a final one, and there is now a race against time to put the DPF in place before the expiration of the six-

Andrew Baer

Chair, Technology, Privacy & Data Security

abaer@cozen.com
Phone: (215) 665-2185
Fax: (215) 372-2400

Related Practice Areas

- Corporate
- Technology, Privacy & Data Security

month grace period that the Irish DPC granted Meta to bring itself into compliance. Complicating matters even further, while it is still likely that the European Commission will approve the DPF, in early 2023, a committee of the European Parliament rejected it as failing to provide essentially equivalent protection, and the EDPB also expressed concerns about a number of issues. Adoption is therefore not assured, and even if approved, the DPF is certain to face a legal challenge on the same grounds as those the court used in *Schrems II*.

Companies engaging in data transfers from the EU to the U.S. should follow these developments closely and review their use of standard contractual clauses and supplementary data protection measures in view of the high bar set by the Irish DPC.

You can learn more information about the Irish DPC's action here.