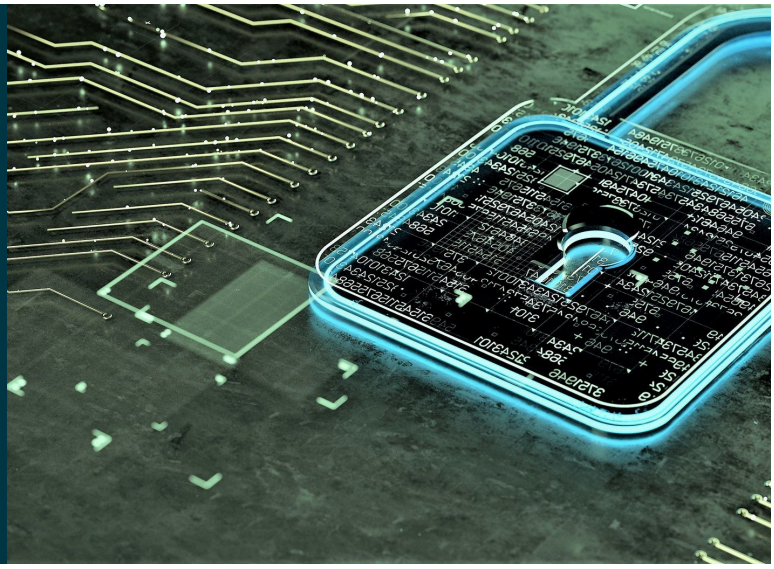
WILSON SONSINI

Meta Receives Record 1.2 Billion EUR Fine and Is Ordered to Suspend Its EU-U.S. Data Transfers



CONTRIBUTORS

Laura De Boel

Sebastian Andre Thess

ALERTS

June 6, 2023

On May 22, 2023, Ireland's Data Protection Commission (DPC) published its long-awaited decision in the Meta EU-U.S. data transfer case (Decision). In its landmark Decision, the DPC imposed a record 1.2 billion EUR fine and ordered Meta Platforms Ireland Limited (Meta) to suspend any EU-U.S. transfers of personal data within approximately five months. Meta was also ordered to bring its operations into compliance within six months. Meta has announced that it will appeal the DPC's decision as well as the underlying decision by the European Data Protection Board (EDPB).

Background

The Decision is the latest twist in the Schrems saga that dates back to the Snowden revelations of 2013. In the wake of those revelations, Austrian privacy activist Maximilian Schrems filed a complaint against Facebook (now Meta) with the Irish DPC (since Meta's EU headquarters is in Ireland). The complaint led to the biggest legal battle in the field of EU privacy law ever. Over the past decade, the proceedings initiated by Schrems have taken many twists and turns, including two cases before the highest court of the EU (CJEU). In both *Schrems I* and *Schrems II*, the CJEU found a lack of adequate protection for EU personal data when it is transferred to organizations in the U.S. subject to U.S. surveillance laws.

In 2022, the DPC submitted its draft decision to order Meta to suspend its EU-U.S. data transfers to the other supervisory authorities (SAs) of the EU. Some SAs, such as the Austrian, German, French, and Spanish SAs, objected and considered that the DPC should take an even tougher stance. The matter was subject to intense debate at the EDPB, which brings together the SAs of the EU member states. Because disagreement remained, the EDPB had to adopt a binding decision under Article 65 GDPR. On April 13, 2023, the EDPB adopted such binding decision requiring the DPC to also order Meta to cease storing personal data that had been transferred from the EU to the U.S., and to impose a substantial fine on Meta.

Key Takeaways from the Decision

1. **Biggest Global Data Protection Regulation (GDPR) fine ever.** The record 1.2 billion EUR fine in the Decision is the result of a strong push by several hardline SAs in the EDPB, and it was imposed by the DPC under pressure from them. This decision fits in the recent trend of increased GDPR enforcement and high fines (such as the 746 million EUR fine that was imposed on Amazon by the Luxembourg SA in 2021).
2. **Grace period may allow Meta to rely on the forthcoming DPF.** In *Schrems II,* the CJEU determined that U.S. surveillance laws, in particular Section 702 of the Foreign Intelligence Surveillance Act (FISA 702) and Executive Order 12333, do not meet EU standards. The EU and U.S. have since worked on a new framework for data flows from the EU to the U.S. A draft of a new "Data Privacy Framework" (DPF) was published by the European Commission (EC) at the end of

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.

2022, and is expected to be formally adopted and become effective later this year. As part of the DPF, the U.S. has committed to strengthening the protection for EU personal data in the U.S. by providing more safeguards for U.S. surveillance activities. Since the new safeguards are not operational yet (and are not intended to apply retrospectively), the DPC considered that they do not impact its assessment of Meta's past and current data transfers. However, the Decision grants Meta a grace period until approximately the end of October 2023 which should allow it to rely on the DPF to bring its data flows into compliance.

3. **No guidance on supplemental measures**. Since *Schrems II*, companies are expected to implement additional safeguards if their data flows are subject to foreign surveillance laws that do not meet EU standards. Meta had implemented such additional safeguards, including organizational, technical (such as encryption in transit), and legal (such as challenging government access requests) safeguards. However, the DPC considered Meta's safeguards insufficient, without offering any suggestions as to what additional measures it should have implemented.
4. **Standard Contractual Clauses remain valid.** Meta had been relying on the EU-approved standard contractual clauses (SCCs) as a legal basis to transfer personal data to the U.S. The DPC did not call into question the validity of the SCCs, but it recalled the CJEU's finding in *Schrems II* that additional safeguards are needed where personal data are transferred to non-EU countries where the data importer would be subject to surveillance laws that do not meet EU standards.

Implications for Organizations Doing Business in the EU

- **Focus on FISA 702.** The Decision applies only to Meta, but it could lead to similar decisions against other organizations doing business in the EU that are also subject to non-EU surveillance programs. In particular, the Decision focuses on FISA 702, which is a U.S. surveillance law that applies to electronic communication providers such as cloud service providers. Many of those organizations need to process EU personal data in the U.S. in order to run their business. In addition, organizations that are not directly subject to FISA 702 are indirectly impacted by this decision, in particular if they rely on cloud service providers that are themselves subject to FISA 702.

  The Decision does not clarify which measures such organizations should take to bring their data flows into compliance. Until the DPF comes into effect, their options will be very limited (e.g., encryption in transit and at rest, data storage in the EU). However, since the Decision focuses on an organization that is directly subject to FISA 702, the risks for other types of organizations are likely lower.

- **Limited utility of Article 49 derogations**. Some organizations may be able to invoke Art. 49 GDPR, which provides for limited derogations from the GDPR's strict data transfer rules. However, the Decision confirms past guidance from EU SAs, which states that those derogations only apply to occasional transfers. In particular, in relation to Article 49.1(a) GDPR (which permits data transfers on the basis of explicit consent), the Decision states that organizations cannot obtain "*a single consent [...] for ongoing data transfers and/or different sets of transfers*." Article 49 GDPR may, therefore, not bring much help.

- **"Data transfer" concept is limited.** Another path forward could be to assess whether all data flows actually fall within the scope of the GDPR's data transfer rules. In 2021, EU SAs clarified that the concept of "data transfer" (which is not defined in the GDPR) does not apply when individuals disclose their personal data directly to an organization on their own initiative. This could give certain B2C organizations leeway to argue that all or part of their data flows are not subject to the GDPR's data transfer restrictions.

- **DPF will be the most solid solution.** For a more solid solution, organizations will need to wait for the DPF to come into effect. The EU is currently waiting for the U.S. to implement the new safeguards that form the basis of the DPF before it issues its DPF adequacy decision. The EU Commission recently stated that it expects the DPF to be in place this summer. Once the DPF is fully implemented, U.S. companies will be able to self-certify their adherence to a set of privacy principles, and on that basis, will be able to transfer EU personal data to the U.S. in compliance with the GDPR. However, the DPF will only apply to EU-U.S. data flows and will not be a basis for data flows to other non-EU countries with surveillance laws that do not meet EU standards.

Conclusion

The Decision shows that transatlantic data transfers increasingly attract regulatory scrutiny in Europe. Until the DPF comes into effect and provides a more solid data transfer solution,

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.

organizations relying on SCCs should consider implementing additional safeguards (e.g., encryption in transit and at rest, data storage in the EU).

Wilson Sonsini Goodrich & Rosati routinely advises clients on GDPR compliance issues, and helps clients manage risks related to the enforcement of global and European data protection laws. For more information, please contact Cédric Burton, Laura De Boel, Maneesha Mithal or another member of the firm's privacy and cybersecurity practice.

Sebastian Thess contributed to the preparation of this Alert.

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.