Transatlantic data transfers: Will new EU-US and UK-US agreements work?

Published 27-Nov-2023 by
Tim Hitchcock

The EU and the United States have finalised the EU-U.S. Data Privacy Framework (DPF), the latest agreement on transferring EU personal information to U.S. entities. A similar UK-U.S. arrangement took effect in October. Large parts of finance depend on processing consumer details digitally, often outsourcing to American data cloud services, but earlier agreements were struck down by European courts.

Schrems I and II

Previous attempts to forge a judge-proof transatlantic data agreement were stymied by European concerns about potential misuse or disclosure of personal information. Some campaigners worry about the Big Techs that dominate cloud computing and social media exploiting information but the two pivotal European Court of Justice (ECJ) rulings concerned actions brought by the activist Max Schrems regarding U.S. security agencies' ability to access Europeans' private data.

The core issue has been whether a data agreement's protection of individuals essentially matches EU protections, especially under the General Data Protection Regulation (GDPR), retained by the UK post-Brexit with small alterations (UK GDPR).

GDPR's salient features are that data processing requires a lawful reason, holders of personal data must obey six general principles, sensitive information carries extra safeguards and data subjects have extensive privacy rights.

The 2015 first Schrems case involved the "Safe Harbor" system. A European Commission decision deemed its protections adequate to allow data transfers to U.S. entities but in Schrems I the ECJ struck down this adequacy decision.

Consequently, the EU and the United States concluded the 2016 Privacy Shield agreement, which the Commission deemed adequate protection and many organisations began making use of EU standard contractual clauses (SCCs).

These are model terms for data transfers to third countries that lack an EU adequacy decision. Max Schrems challenged this situation.

In the 2020 second Schrems case, the ECJ ruled on the Privacy Shield and the use of SCCs. It struck down the Privacy Shield for not providing essentially equivalent protections to the GDPR and EU Charter of Fundamental Rights (CFR).

This was because U.S. surveillance programmes were a disproportionate interference with privacy rights, against which there was no effective judicial protection. The ECJ upheld SCCs but said they must include terms providing essentially equivalent protections to GDPR and CFR.

Data Privacy Framework

The new DPF, which received its Commission adequacy decision on July 10, must overcome the obstacle of the Schrems II judgment.

Whether it fares better than its predecessors may depend on its central feature: a U.S. commitment to enhancing safeguards regarding its intelligence activities contained in an Oct. 7, 2022 White House executive order (the EO).

"The EO addressed concerns raised by the ECJ in Schrems II, including the lack of necessity and proportionality constraints on U.S. surveillance and insufficient redress rights for EU citizens to challenge unlawful surveillance practices," said Paul Kavanagh, head of the law firm Dechert's intellectual property team in London.

"As the successor to the Privacy Shield, the DPF incorporates the EO and consequently adopts a more stringent approach toward the access of U.S. intelligence authorities to EU citizens' personal data."

By incorporating the EO, the DPF also enhances the redress mechanisms available to individuals in the EU. The EO caused the establishment of the independent Data Protection Review Court, whose role is to examine and address complaints about access to EU citizens' data in the course of U.S. signals intelligence activities.

Eligible U.S. outsourcing or cloud data storage service providers can choose to self-certify that they adhere to the DPF and their commitment is enforceable under U.S. law by the relevant authority, including the Federal Trade Commission.

Financial services firms that store European personal information using a U.S. service provider can check whether it has signed up to the DPF on the federal government's DPF participants list.

"If U.S. vendors engaged by financial services firms are DPF-certified, they will not need to obtain SCCs or other transfer mechanisms," Kavanagh said.

"However, unlike SCCs, the DPF does not incorporate Article 28 GDPR terms [on outsourcing data processing] into data transfers. Therefore, even where U.S. data vendors are DPF-certified, data processing agreements that meet the requirements of Article 28 GDPR will still be necessary."

Data Bridge

The UK's agreement, the Data Bridge, deems U.S. protections adequate where a UK-based organisation transfers data to a U.S.-based one that is listed as participating in the UK extension to the DPF. The Data Bridge was implemented by the Data Protection (Adequacy) (United States of America) Regulations 2023, which took effect on Oct. 12.

The data protection regimes in the EU and UK are largely similar, as are the protections under the DPF and Data Bridge, but firms should be aware that there are differences, Kavanagh said.

"For example, the 'sensitive information' definition under the Data Bridge does not mirror the definition of 'special categories of personal data' as per the UK GDPR," Kavanagh said.

"Therefore, when transferring data to a U.S. organisation certified under the Data Bridge, UK businesses will need to specifically designate certain types of data as 'sensitive'."

The attraction of making U.S. data transfers under the DPF or Data Bridge should be that processes are faster and costs lower than using SCCs. There would be no need to make an expensive data transfer impact assessment (TIA).

These are required due to the Schrems II decision's observations about SCCs and in effect certify that data transferred to a third country would have essentially equivalent protections under its laws as in the EU or UK.

On the other hand, the investment firms have made in TIAs and the other requirements for making transfers under SCCs may deter them from taking a chance on the DPF surviving when Safe Harbor and Privacy Shield did not.

They may be especially unwilling to ditch cumbersome but reliable SCCs having had to overhaul those contracts recently.

Following Schrems II, the European Commission issued modernised SCCs under GDPR in 2021. Existing contracts had to be migrated to the new form by Dec. 27, 2022. The UK Information Commissioner's Office (ICO) has replaced SCCs with an international data transfer agreement (IDTA) for the UK to third-country transfers.

It also issued an addendum that firms can use with modernised SCCs to show compliance with the UK GDPR. UK firms must replace the existing SCC with the IDTA or the addendum by March 21, 2024.

Uncertain future

There are already doubts about the durability of the EU and UK's new arrangements with the United States. The ICO's opinion on the Data Bridge noted that differences between UK and U.S. law could diminish protections for UK data subjects.

"The Data Bridge does not contain rights that are substantially similar to the right to be forgotten under the UK GDPR, nor does it provide an unconditional right to withdraw consent," Kavanagh said.

"The Data Bridge also does not specify all the special categories of personal data under the UK GDPR."

As for Max Schrems, a not-for-profit organisation he founded called NOYB (standing for "none of your business") has said it will challenge the DPF. NOYB expects to be before the ECJ in early 2024 and says the court could suspend the DPF while it reviews it.

"The future of the DPF and the Data Bridge remains uncertain," Kavanagh said.

(Tim Hitchcock, for Regulatory Intelligence)

Complaints Procedure

Produced by Thomson Reuters Accelus Regulatory Intelligence 27-Nov-2023