

C L I F F O R D
C H A N C E

**EUROPEAN COMMISSION APPROVES
EU-U.S. DATA PRIVACY FRAMEWORK**

EUROPEAN COMMISSION APPROVES EU-U.S. DATA PRIVACY FRAMEWORK

On 10 July 2023, the European Commission (“EC”) reached an “[adequacy decision](#)” under the European Union (“EU”) General Data Protection Regulation (“GDPR”), approving transfers of personal data to organisations located in the United States (“U.S.”) that will be certified under the newly-established Trans-Atlantic Data Privacy Framework (“DPF”) agreed between the U.S. and the EU.

This long-awaited decision replaces the EU-U.S. “Privacy Shield”, which was invalidated by the Court of Justice of the European Union (“CJEU”) in the *Schrems 2* case in 2020 (see our [article](#) on *Schrems 2*). Although the adequacy decision is likely also to be challenged before the CJEU, for the time being the decision dispels the considerable uncertainty around transfers of personal data regulated by the EU GDPR to the U.S. that arose following *Schrems 2*. It should greatly simplify the risk analysis associated with these transfers, even where they are made to U.S. recipients which do not participate in the DPF. Businesses will need to review their compliance strategies to explore taking advantage of the opportunities presented by the DPF and EU adequacy decision.

Background

The GDPR regulates the circumstances in which personal data can be transferred to countries outside the EEA. The starting point (with exceptions) is that transfers may only be made to countries which the EC has decided (pursuant to Article 45(3) GDPR) ensure “adequate protection” (or, in the CJEU’s words, an “essentially equivalent” level of protection) for the transferred personal data. The EC has made adequacy decisions in relation to various countries with relatively strict data protection regimes – for example, Argentina, Japan and the UK. It has also historically made a series of adequacy decisions in relation to the U.S., of which the DPF is the third and latest.

The U.S. does not have a data privacy regime of general application, so the adequacy decisions in respect of transfers between the EEA and the U.S. have applied only to transfers to U.S. organisations which make a public commitment to comply with a set of data privacy principles, broadly similar to the substantive principles of EU data protection law, which are overseen and enforced by the U.S. Federal Trade Commission (“FTC”) and Department of Transportation (“DOT”).

The first two of these adequacy decisions – the “Safe Harbor” framework and “Privacy Shield” – were both previously invalidated by the CJEU on the basis that, although their stated data privacy principles are laudable, they were substantively undermined by the U.S. federal laws empowering U.S. governmental agencies to demand access to information. While EU law will, of course, accept that there are circumstances in which governmental agencies should properly be able to demand access to information held in the private sector, the CJEU took the view that U.S. law as it then stood did not include sufficient checks and balances on these access rights to allow the Safe Harbor framework or Privacy Shield to deliver the required “essentially equivalent” level of protection to that provided by EU law.

The *Schrems 2* case, which invalidated Privacy Shield, also took a nuanced view on the other key international data transfer mechanism under the GDPR – that is, the use of standard contractual clauses (“SCCs”), in the form approved by the EC and put in place between an EEA transferor (called an Exporter) and a third country transferee (called an Importer), to protect transferred personal data. In *Schrems 2* the CJEU accepted the possibility of relying on SCCs, but only subject to the transferor having satisfied itself, through a so-called transfer impact assessment (“TIA”), that they will deliver an essentially equivalent level of protection to that guaranteed by EU law. (The CJEU in *Schrems 2* did not consider the status of the *other* key international data transfer mechanism in the GDPR – so-called “binding corporate rules” (“BCRs”) put in place within an international corporate group to protect intra-group transfers and approved by the relevant data protection supervisory authorities – but the applicable principles are essentially the same.)

The combined effect of the invalidity of Privacy Shield and the need to conduct TIAs (and reach positive conclusions) when relying on SCCs (or BCRs) has been to create considerable uncertainty as to the circumstances in which personal data can lawfully be transferred from the EEA to the U.S. The Irish Data Protection Commissioner has, for example, recently decided that transfers of Facebook data made by Meta Ireland to Meta U.S. on the basis of the EC’s SCCs are (or at least were, before the changes discussed in this article) not in line with the GDPR.

The trans-atlantic data privacy framework

The EC adequacy decision exercises a power of the EC under the GDPR to determine that a third country ensures adequate protection for personal data, subject to a process of consultation with (amongst others) the European Data Protection Board (“EDPB”, the college of EU data protection supervisory authorities) and the European Parliament, and support by a qualified majority of the EU Member States. In this case, 24 out of the 27 Member States approved the decision, the other three abstaining.

The effect of the decision is to allow transfers of personal data to U.S. organisations which have self-certified that they will comply with a set of data privacy principles. The principles are functionally identical to those of Privacy Shield. Self-certifying organisations will be identified in a list which is to be published and maintained by the U.S. Department of Commerce (“DOC”). The EC has decided that the U.S. ensures adequate protection, but only where personal data is transferred to one of these self-certifying organisations.

The DPF's data privacy principles are complemented by changes in (and other U.S. commitments regarding) U.S. law on governmental access to information (see our [article on the Data Protection Framework](#)). The changes, made through U.S. Executive Order 14086 and related regulations, policies and procedures, newly require U.S. government agencies to demand access to information relating to individuals only when necessary for and proportionate to defined national security purposes; and they give individuals in so-called "Qualifying States", which include all the Member States of the EU and the wider EEA, enhanced rights of redress, including through a newly established court known as the "Data Protection Review Court", if they are concerned about possible abuse of their data privacy rights.

The adequacy decision will not take effect until a mechanism is available for self-certification to the DPF and U.S. organisations have been through the self-certification process and appear in the DOC's published list. Details of the self-certification process are not yet available (see <https://www.dataprivacyframework.gov/s/> - the site is planned to become accessible from 17 July 2023), but organisations already participating in Privacy Shield (which remains "open" although it has not been recognised under EU law as an effective transfer mechanism since 2020) will be able to swiftly port over to the DPF.¹ Transfers to those organisations, and others self-certifying under the DPF in the future, will then be able to go ahead without breach of the GDPR's international personal data transfer restrictions. Importantly, the EU and EEA data protection supervisory authorities (individually or collectively in the form of the EDPB) do not have the power to override the adequacy decision, other than by reference to their national courts and on to the CJEU.

One point to note is that the DPF, like both the Safe Harbor framework and Privacy Shield before it, is only available to U.S. organisations regulated by the FTC or DOT. Other organisations – notably banks and some other types of financial institutions – will not be eligible to participate and will therefore need to continue to rely on SCCs (or BCRs) for their intra-group transfers and other transfers to their U.S. operations. U.S. organisations outside the DPF will, however, be able to rely on the DPF when they make "onward" transfers of EU / EEA personal data to DPF-participating service providers (or others) in the U.S.

Implications for transfers outside the DPF

The most significant differences between the DPF and Privacy Shield lie not in the data privacy principles to which DPF participants commit themselves but in the associated changes in U.S. law on governmental access to information. These changes apply generally, not only to information held by DPF participants. In principle, therefore, they should have implications for reliance on the EC's SCCs, and on BCRs, which are as significant as the DPF itself. The EC has in effect decided that the deficiencies of U.S. law identified in *Schrems 2* have been fully addressed, leaving little, if any, scope for an EU or EEA supervisory authority to conclude (other than through a reference to the CJEU) that the SCCs or an approved set of BCRs do not deliver essentially equivalent

¹ [Guidance issued by the DOC](#) indicates that current participants in Privacy Shield can rely on the adequacy decision immediately, without the need to re-certify, provided they update their privacy policies accordingly by 10 October 2023. According to the terms of the adequacy decision itself they cannot rely on the decision until they are identified in a "Data Privacy Framework List" published by the DOC. No such list has been published as at the date of this article, but presumably it will be published shortly.

protection for personal data transferred to the U.S. When relying on SCCs, a TIA will still be necessary in principle, but – unless there are further changes in U.S. law which muddy the waters in the future – it will substantially just repeat the analysis already carried out by the EC and set out in the adequacy decision. This should be the case, with only limited potential for exceptions, even where transfers are made to U.S. organisations which are not eligible to participate in the DPF.

What about the UK?

The adequacy decision does not directly affect transfers of personal data which are subject to the UK version of the GDPR. However, the U.S. proposes to launch a UK extension to the DPF on 17 July 2023. It will not become effective until the UK reaches an appropriate adequacy decision, but that is expected soon thereafter.

There will be similar arrangements for transfers from Switzerland.

Challenge

Max Schrems, the privacy advocate who brought the cases leading to the invalidation of the Safe Harbor framework and Privacy Shield, has already announced that he does not accept that the DPF delivers the required essentially equivalent level of protection of personal data regulated by the GDPR and will seek to persuade the CJEU to invalidate the adequacy decision. The process will be lengthy – years, rather than months – and the outcome is inevitably uncertain.

Practical implications

- U.S. organisations which receive transfers of EU / EEA / UK personal data will need to decide whether to self-certify under the DPF and, if so, review and pursue the new certification process when it becomes available. Bear in mind that not all U.S. organisations will be eligible to participate. Some eligible U.S. organisations may prefer not to self-certify but rather to rely on SCCs and/or BCRs.
- EU / EEA / UK organisations transferring personal data to the U.S. in reliance on the SCCs might consider instead relying on the DPF, where they are transferring personal data to DPF participants. They might now be making enquires of their U.S. service providers.
- International groups of organisations will need to consider these questions from both perspectives.
- UK organisations should keep track of developments towards a UK equivalent of the DPF.
- Existing TIAs for transfers to the U.S. may need to be reviewed. They will no longer be necessary where transfers are made to a DPF participant, and in other cases it should be possible to simplify their U.S. legal analysis based on the adequacy decision. Organisations subject to the GDPR may take the existence of the DPF as evidence that the conclusions of their transfer risk assessments are defensible.
- It will be important to follow the likely challenges to the DPF adequacy decision and be prepared to revert to SCCs, if necessary, in the future.
- In respect of transfers to countries which *do not* benefit from adequacy decisions, it generally remains necessary to rely on the SCCs and/or BCRs, except in rare cases where derogations allow transfers to take place.

CONTACTS



Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com



Devika Kornbacher
Partner
Houston
T: +1 713 821 2818
E: devika.kornbacher@cliffordchance.com



Jonathan Kewley
Partner
London
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com



Stella Cramer
Partner
Singapore
T: +65 6410 2208
E: stella.cramer@cliffordchance.com



Simon Persoff
Partner
London
T: +44 207006 3060
E: simon.persoff@cliffordchance.com



Richard Jones
Director of Data Privacy
London
T: +44 207006 8238
E: richard.jones@cliffordchance.com



Megan Gordon
Partner
Washington DC
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com



Daniel Silver
Partner
New York
T: +1 212 878 4919
E: daniel.silver@cliffordchance.com



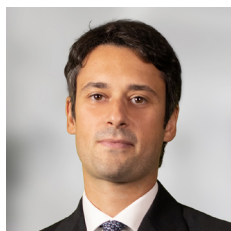
Holger Lutz
Partner
Frankfurt
T: +49 69 7199 1670
E: holger.lutz@cliffordchance.com



Ines Keitel
Partner
Frankfurt
T: +49 69 7199 1250
E: ines.keitel@cliffordchance.com



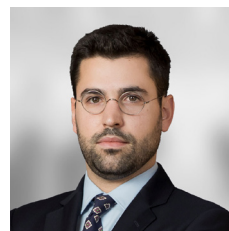
Gunnar Sachs
Partner
Dusseldorf
T: +49 211 4355 5460
E: gunnar.sachs@cliffordchance.com



Andrea Tuninetti Ferrari
Lawyer - Counsel
Milan
T: +39 02 8063 4435
E: andrea.tuninettiferrari@cliffordchance.com



Andrei Mikes
Counsel
Amsterdam
T: +31 20 711 9507
E: andrei.mikes@cliffordchance.com



Manel Santilari
Abogado
Barcelona
T: +34 93 344 2284
E: manel.santilari@cliffordchance.com



Brian Yin
Associate
New York
T: +1 212 878 4980
E: brian.yin@cliffordchance.com

CLIFFORD CHANCE

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2023

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.