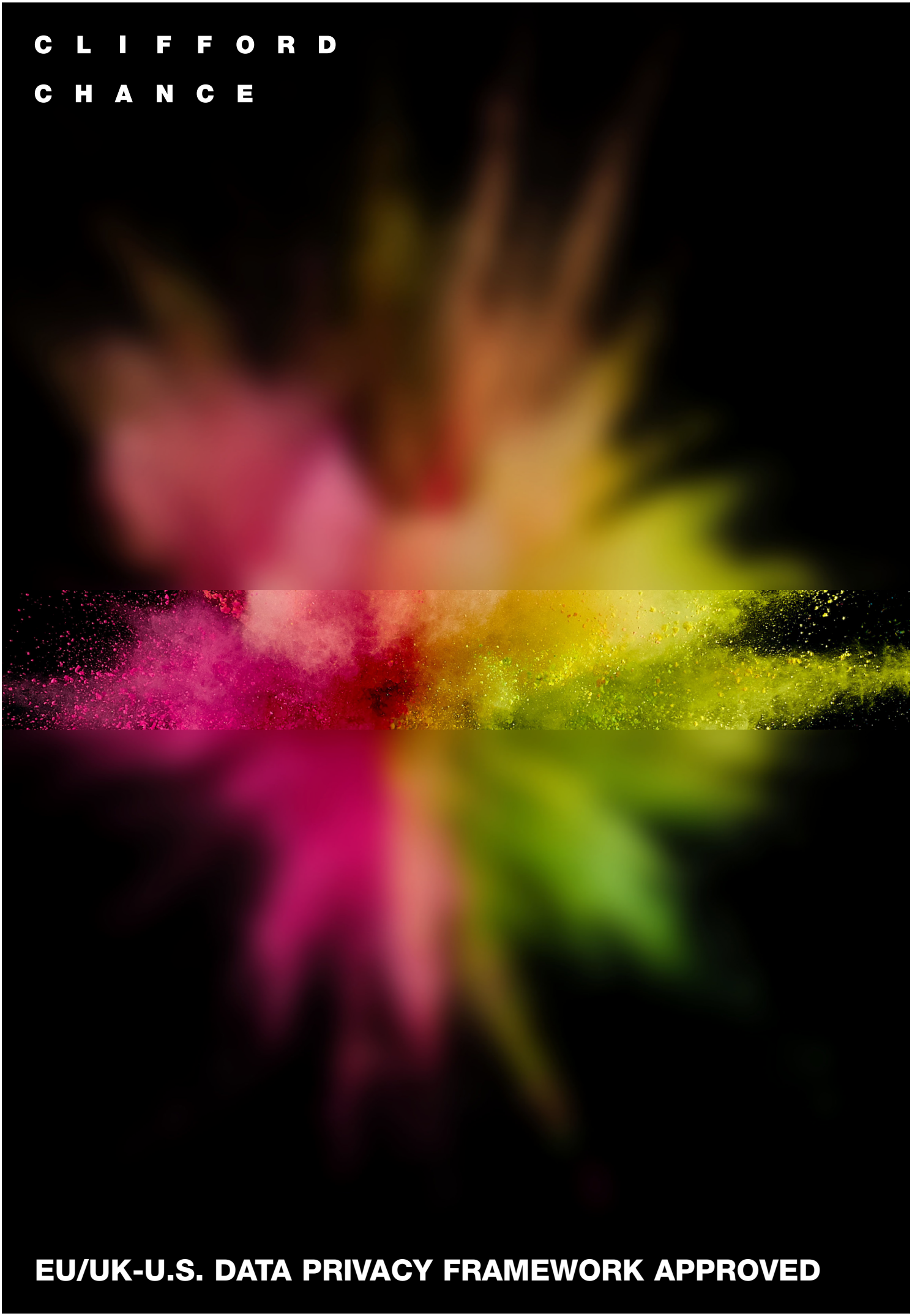
CLIFFORD

CHANCE



EU/UK-U.S. DATA PRIVACY FRAMEWORK APPROVED

EU/UK-U.S. DATA PRIVACY FRAMEWORK APPROVED

This article was first published in July 2023. It was re-published, expanded to cover the UK approval of the framework, in September 2023.

On 10 July 2023, the European Commission ("EC") reached an "adequacy decision" under the European Union ("EU") General Data Protection Regulation ("EU GDPR"), approving transfers of personal data to organisations located in the United States ("U.S.") that are certified under the newly-established Trans-Atlantic Data Privacy Framework ("DPF") agreed between the U.S. and the EU. On 12 October 2023, an equivalent decision, in respect of the same DPF, will take effect for the purposes of the ***UK*** General Data Protection Regulation ("UK GDPR" and, together with the EU GDPR, "GDPR"). The UK Government prefers to refer to the DPF as a "data bridge".

These long-awaited decisions replace 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 decisions are likely also to be challenged before the CJEU and the UK courts, for the time being they dispel the considerable uncertainty around transfers of personal data regulated by the GDPR to the U.S. that arose following *Schrems 2*. They 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 the adequacy decisions.

Background

The GDPR regulates the circumstances in which personal data can be transferred to countries outside the EEA / UK. The starting point (with exceptions) is that transfers may only be made to countries which the EC (under the EU GDPR) or a UK Government minister (under the UK GDPR) has decided ensure "adequate protection" (or, in the CJEU's words, an "essentially equivalent" level of protection) for the transferred personal data. Adequacy decisions have been made in relation to various

countries with relatively strict data protection regimes – for example, Argentina, Japan and Switzerland - and the EU and UK have each made adequacy decisions in relation to the other. The EC 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 previously made in respect of transfers between the EEA and the U.S. applied only to transfers to U.S. organisations which made a public commitment to comply with a set of data privacy principles, broadly similar to the substantive principles of EU data protection law, which were 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 were laudable, they were substantively undermined by U.S. federal laws empowering U.S. governmental agencies to demand access to information. While EU and UK law will, of course, accept that there are circumstances in which governmental agencies should properly be able to access 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 EU 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 would deliver an essentially equivalent level of protection to that guaranteed by EU law. A similar view is taken under the UK GDPR. (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 or UK 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 EU GDPR.

The trans-atlantic data privacy framework

The EC and UK adequacy decisions exercise powers under the GDPR to determine that a third country ensures adequate protection for personal data, subject, in the case of the EU GDPR, to a process of consultation with (amongst others) the European Data Protection Board (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 UK decision was able to be made more simply, by regulations made by a UK Government minister after consultation with the UK Information Commissioner's Office ("ICO").

The effect of the decisions 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 are identified in a list which is published and maintained by the U.S. Department of Commerce ("DOC"). The EC and the UK have 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 EU/EEA Member States and the UK, enhanced rights of redress, including through a newly established court {the "Data Protection Review Court"), if they are concerned about possible abuse of their data privacy rights.

The U.S. Government has established and published a process through which U.S. organisations can self-certify under the DPF. They can choose whether to participate in the "UK" as well as the "EU" version of the DPF, but cannot participate only in the UK version (known as the "UK extension"). U.S. organisations that were participating in the Privacy Shield when the EU adequacy decision took effect were automatically ported into both the EU and the UK versions of the DPF. The substantive requirements of the EU and the UK versions are exactly the same. Transfers to participating organisations can go ahead without breach of the GDPR's international personal data transfer restrictions, the Exporter's responsibility being limited to checking that the Importer is identified in the relevant part of a list published by the DOC and that its published certification covers the transferred data. Importantly, the EU/EEA/UK data protection supervisory authorities do not have the power to override the adequacy decisions, other than by reference to their national courts and (in the case of EEA authorities) 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 / UK personal data to DPF-participating service providers (or others) in the U.S.

Note further that guidance issued by the UK Government in relation to the UK adequacy decision indicate some limitations on the scope of the decision. In particular:

- The DPF principles do not apply to personal data collected for journalistic purposes. The UK Government takes the view – although this is not reflected in the UK decision itself, nor in the EC's equivalent decision – that the decision does not allow transfers to the U.S. of personal data in this category.

- Certain specific categories of data, which are treated as particularly sensitive under the GDPR, are only treated as sensitive under the DPF principles if the Exporter informs the Importer of their sensitivity. The UK Government appears to take the view that the principles do not provide adequate protection for transferred personal data in these categories unless the Exporter has informed the Importer of their sensitivity. This applies to genetic data, biometric data processed for the purposes of uniquely identifying a natural person, data concerning sexual orientation and data relating to criminal convictions and offences or related security measures. Again, this view is not reflected in the decision itself, nor in the EC's equivalent decision -although it may be that transfers of, for example, biometric data would breach Article 9 of the UK GDPR if they are made without informing the Importer of their sensitivity.

It remains to be seen whether the ICO and courts would support these positions, and whether similar views may be adopted by EU/EEA data protection supervisory authorities.

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 their UK equivalents), and on BCRs, which are as significant as the DPF itself. The EC has in effect decided, and an equivalent decision has effectively been made under UK law, that the deficiencies of U.S. law identified in *Schrems 2* have been fully addressed, leaving little, if any, scope for an EU / EEA or UK supervisory authority to conclude (other than through a reference to the CJEU or the UK courts) that the SCCs or an approved set of BCRs do not deliver essentially equivalent 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 built into the adequacy decisions. 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 Switzerland?

There are similar arrangements for transfers from Switzerland, but they fall outside the scope of this article.

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 EU 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. A similar challenge to the UK decision may conceivably be made through the UK courts, although they are not bound to follow any CJEU decision. There is also the possibility that, if the EU decision is invalidated but the UK decision is not, a challenge might then be made to the EC adequacy decision covering transfers of personal data ***to the UK***, on the basis that the UK DPF decision amounts to a failure to provide essentially equivalent protection for personal data transferred from the EEA.

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. 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.
- 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
Tech Group
Knowledge – UK
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

www.cliffordchance.com

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

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.

2307-007016