ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy ADVISORY ■

SEPTEMBER 7, 2023

EU-U.S. Data Privacy Framework vs. EU Standard Contractual Clauses for Transatlantic Transfers of Personal Data

by *Paul Greaves* and *Wim Nauwelaerts*

The Story So Far

On July 10, 2023, the European Commission (EC) adopted its long-awaited adequacy decision approving the EU-U.S. Data Privacy Framework (DPF). By doing so, the EC confirmed that personal data transferred to the United States under the DPF is adequately protected in line with the rules on international data transfers imposed by the EU General Data Protection Regulation (GDPR). As we discussed in our July 12, 2023 blog post, companies established in the EU (or whose personal data processing is otherwise subject to the GDPR) can now transfer personal data to the United States under the DPF.

Companies that need to transfer personal data from the EU to the United States are now faced with an important decision: Does it make sense to use the DPF, or is it better to leverage one of the other transfer tools available under the GDPR, such as the EU's Standard Contractual Clauses (SCCs)?

The DPF vs. the SCCs: Key Distinction

Before diving into the similarities and differences in more detail, it is important to bear in mind one significant distinction: The DPF can only be used for transfers of personal data to the United States, whereas the SCCs can in principle be used to transfer personal data from the EU to any third (non-EU) country (subject to the requirement to carry out a transfer impact assessment (TIA)). Global companies that decide to use the DPF for transfers of personal data to the United States may therefore also need to use the SCCs for transfers to other jurisdictions.

Our analysis of the SCCs assumes that the transfers of personal data are to recipients in the United States only.

Transfer Impact Assessments: Just One Piece of the Compliance Puzzle

One requirement for using the SCCs has attracted renewed attention since the EC approved the DPF: the need to carry out and document a TIA before using the SCCs.

A TIA involves assessing whether personal data will be appropriately protected when it has been transferred to a third country, taking into account (1) the specific circumstances of the transfer of personal data; (2) the laws and practices in the third country (including those requiring the disclosure of data to public authorities or authorizing access by such authorities); and (3) additional safeguards put in place to protect the data.

The European Data Protection Board has confirmed that companies using the DPF (instead of the SCCs) do not need to perform a TIA. This is, of course, one factor weighing in favor of the DPF.

However, it is important to consider this in context. The need to carry out a TIA is just one of the many requirements for using the SCCs. Regardless of whether a company uses the DPF or the SCCs, each data transfer tool has a broader set of compliance requirements to consider and implement as needed. For the DPF, participant organizations must self-certify that they comply with the data protection principles of the DPF. For SCCs, the compliance requirements are underpinned by contractual obligations between the parties (i.e., the data exporter and the data importer) aiming to safeguard personal data after it has been transferred.

The applicable requirements under the SCCs depend on which module of the SCCs is being used for the transfer in question. For example, the obligations under Module 1 (used for controller-to-controller transfers) are different from those under Module 2 (used for controller-to-processor transfers).

Using Module 1 as an example, it is clear that the compliance requirements imposed by the SCCs are similar to those that apply under the DPF:

> **Transparency requirements.** Under the DPF's 'Notice' principle, participating organizations must inform individuals whose personal data is transferred to the United States of the types of personal data transferred and, when applicable, the other entities or subsidiaries of the organization that are also adhering to the principles. Similarly, under Clause 8.2 (Transparency) of Module 1 of the SCCs , the data importer is responsible for providing individuals with specific information regarding the transfer, including the importer's identity and contact details, as well as the categories of personal data processed.
>
> **Data subject rights requirements.** Under the DPF's 'Access' principle, individuals have the right to obtain access to personal data about them, and they can also ask to correct, amend, or delete that data if it is inaccurate or if it has been processed in violation of the DPF's principles. Similarly, under Clause 10(a) (Data Subject Rights) of Module 1 of the SCCs , the data importer must deal with any inquiries and requests it receives from individuals on the processing of their personal data and the exercise of the data protection rights awarded to them by the GDPR.
>
> **Redress/recourse requirements.** The DPF's 'Recourse, Enforcement and Liability' principle requires participating organizations to ensure that there are robust mechanisms for assuring compliance with the principles; recourse for individuals who are affected by noncompliance with the principles; and consequences for the organization when the principles are not followed. The mechanisms must include readily available independent recourse mechanisms for investigating and expeditiously resolving each individual's complaints and disputes. The SCCs, on the other hand, contain their own

set of redress requirements, notably under Clause 11 (Redress), which, for example, requires the data importer to inform individuals in a transparent and easily accessible format, through individual notice or on a website, of a contact point authorized to handle complaints. The data importer must also deal promptly with any complaints it receives from individuals whose personal data it has imported.

How Can Companies Make the Right Choice?

It is important to consider the substantial differences between the SCCs and the DPF. The following table highlights some of the differences to consider when choosing between the SCCs and the DPF.

KEY FEATURES	SCCs	DPF
Scope of application	The SCCs can in principle be used to transfer personal data from the EU to any third country.	The DPF can only be used for transfers of personal data from the EU to the United States.
Ability to apply the tool to UK/Swiss data transfers	It is possible to use the SCCs for transfers of personal data protected by UK and Swiss data protection laws by attaching country-specific addenda to the SCCs. Companies can therefore align their EU, UK, and Swiss transfer practices by using one data transfer tool (i.e., the SCCs).	There are plans to enable companies to use the DPF for transfers of personal data protected by UK and Swiss data protection laws. However, that is not possible yet.
Primary means of commitment	The SCCs must be executed between or on behalf of each exporter and importer of personal data. This can result in a heavy compliance burden (for example, when a global company with many affiliates uses the SCCs to cover all of its intragroup transfers of personal data).	Companies adhere to the DPF by self-certifying with the U.S. Department of Commerce and by paying an annual fee. There is no specific requirement to enter into agreements as between exporters and importers for the DPF to be effective.
Need to implement additional agreements	By signing the SCCs, exporters and importers enter into a binding agreement that governs the transfer and processing of personal data. In addition, Modules 2 and 3 of the SCCs already cover the processor requirements imposed by Article 28 of the GDPR. Therefore, in many cases no additional data processing agreement is needed.	The DPF does not cover the requirements imposed by Article 28 of the GDPR. U.S. companies using the DPF and acting as processors for controllers in the EU may therefore need to enter into additional data processing agreements.

KEY FEATURES	SCCs	DPF
Ease of demonstrating compliance	There is no publicly available register showing that a company has put in place SCCs.	If a company self-certifies to the DPF, third parties can easily verify that the company adheres to the DPF (or at least purports to do so) by checking that the company's name appears on the publicly available register at https://www.dataprivacyframework.gov/s/. This can be of persuasive value when dealing with vendors, partners, or other third parties who may ask companies to demonstrate compliance with EU data transfer rules.
Need to monitor regulatory developments/conduct a TIA	Since there is a requirement to perform a case-by-case TIA when using SCCs, companies will need to keep an eye on regulatory and legal developments and, if necessary, adjust their practices. Existing TIAs may also need to be updated if the relevant U.S. laws and practices change.	No need to conduct a TIA when using the DPF. When a company joins the DPF, it will likely be able to continue to transfer personal data to the U.S. until such time that the DPF is invalidated (if and when that happens - see below). This provides a level of certainty for such companies' transfers of personal data to the U.S. in the medium term.
Future challenges to effectiveness	It would be theoretically possible to challenge the validity of the SCCs in their current format, however we are not aware of any credible or high-profile challenges. By contrast, an individual or a supervisory authority can challenge a company's particular use of the SCCs if they consider the specific transfer of personal data to be problematic.	Privacy activists in the EU have already indicated that they plan to challenge the validity of the new DPF. However, a legal challenge to the DPF is likely to take time.

Conclusion

Despite some underlying similarities between the DPF and the SCCs, there are important differences in the upfront investment required and the ongoing compliance burden. Companies seeking to choose between these transfer tools should consider each with an open mind, taking into account the above factors as well as other elements that may be material to the company's particular circumstances and needs.

You can subscribe to future ***Privacy, Cyber & Data Strategy*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or a member of our **Privacy, Cyber & Data Strategy Team**:

Paul Greaves
+32 2 550 3791
paul.greaves@alston.com

Wim Nauwelaerts
+32 2 550 3709
wim.nauwelaerts@alston.com

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 4th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 755 Page Mill Road ■ Building C - Suite 200 ■ Palo Alto, California, USA 94304-1012 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333