**LEGAL ALERT**

**Re:** **United States - European Union Data Privacy Framework**

This Alert provides background information and operational advice regarding the European Union and United States Data Privacy Framework (“EU-US DPF” or “Framework”) which became effective on July 10, 2023. The cross-border transfer of personal data is a fundamental underpinning of commerce and investment between the US and the EU. The EU-US DPF facilitates data flows between EU member states and the US while protecting individual rights and personal data of EU residents. The new Framework ends an extended period of legal uncertainty for companies that rely on freely transferring data between the EU and the US.[[1]](#footnote-1) However, future questions remain about whether the EU-US DPF will withstand a pending challenge within the EU judicial system.

We are providing this information to ensure that stakeholders in the assessment and learning industry understand the importance and implications of these recent events.

1. **Background**

Since its adoption in 2018, the EU General Data Protection Regulation (GDPR) has prohibited transfers of data outside of Europe in the absence of adequate safeguards which ensure a comparable level of protection of personal data – a so-called “adequacy ruling.” Two former agreements negotiated between the EU and the US regarding the cross-border flow of data were invalidated by the European Union’s highest court, the Court of Justice of the European Union (CJEU), largely because the Court determined that the US intelligence laws do not provide adequate privacy protections for EU residents. The most recent agreement, known as Privacy Shield, was invalidated in 2020 after the CJEU determined it did not include enough privacy protections (the Schrems II decision).

The lack of a formal bi-lateral agreement covering cross-border data transfers since 2020 has caused tremendous uncertainty for US companies who rely on the free flow of data between the EU and the US. Without a regulatory solution, US companies have been forced to use other mechanisms to address

the problem, either through the use of Standard Contractual Clauses or Binding Corporate Rules.[[2]](#footnote-2) SCCs are a**“ready-made”** and easy-to-implement tool for companies that may not have the resources to negotiate individual contracts with each of their commercial partners. SCCs are also distinguished from other compliance mechanisms that require prior authorization by a national data protection authority (e.g., ad hoc contracts for data transfers) or are typically more costly to implement (e.g., certification schemes). Feedback from stakeholders shows that SCCs are by far the **most used data transfer instrument** for European companies. For example, according to the IAPP-EY Annual Privacy Governance Report 2019, “the most popular of these [transfer] tools – year over year – are overwhelmingly standard contractual contracts: 88% of respondents in this year’s survey reported SCCs as their top method for extraterritorial data transfers […]” However, the same has not been generally true for smaller US companies because these mechanisms are cumbersome and entail significant legal cost. In spite of approved SCCs, European privacy regulators have fined major US technology firms billions of euros for improperly sending the data of EU citizens to the US.[[3]](#footnote-3) In light of these problems and uncertainty, the US Department of Commerce spearheaded negotiations with the European Union to replace the invalidated Privacy Shield with a new agreement addressing the issues raised by the CJEU. This new agreement is called the EU-US Data Privacy Framework.

On October 7, 2022, President Joe Biden issued Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence. EO 14086 was tailored to address the findings from the CJEU which invalidated Privacy Shield. These findings center on proportionality and redress. First, EO 14086 requires US intelligence agencies to collect only information proportionate to associated national security risks.[[4]](#footnote-4) Complaints will be investigated by the so-called ‘Civil Liberties Protection Officer'[[5]](#footnote-5) of the US intelligence community. This person is responsible for ensuring compliance by US

intelligence agencies with privacy and fundamental rights.  Second, EO 14086 established an independent review body made up of American judges, known as the Data Protection Review

Court, which has the power to investigate and resolve complaints regarding access to their data by US national security authorities, to allow Europeans to object when they believe their personal information has been collected via improper means by US intelligence agencies.[[6]](#footnote-6) This redress mechanism was established to satisfy the findings from the Schrems II decision.

1. **Adequacy Decision**

Culminating the extensive negotiations over a new process, the European Commission adopted an adequacy decision formally approving the EU-US DPF on July 10, 2023[[7]](#footnote-7). The adoption of the adequacy decision indicates that based on the implementation of the EU-US DPF, the US is now considered to offer a level of personal data privacy protection aligned with GDPR requirements. In short, the European Commission adequacy decision gives the green light to companies wishing to transfer personal data from Europe to the US by relying on the EU-US DPF.

As a result of adequacy decisions, personal data can flow freely and safely from the European Economic Area (EEA), which includes the 27 EU Member States as well as Norway, Iceland, and Liechtenstein, to a third country, without being subject to any further conditions or authorizations. In other words, transfers to the US can be handled in the same way as intra-EU transmissions of data.

1. **Future Legal Challenge**

The same day the European Commission issued its adequacy decision approving the DPF, the Austrian privacy activist Max Schrems and his advocacy organization None of Your Business (NOYB) announced plans to sue over the validity of the new agreement. Two previous cases, known as Schrems I and Schrems II, invalidated the former Safe Harbor and Privacy Shield agreements, respectively. Now, NOYB and Schrems assert that the changes made under EO 14086 are not substantive enough to withstand a CJEU challenge; instead, they have called for changes in U.S intelligence gathering/surveillance laws.

Future changes in U.S surveillance laws are considered unlikely.[[8]](#footnote-8) Accordingly, the forthcoming legal challenge to the Framework will result in a lengthy period of uncertainty surrounding its legal status until the CJEU issues a final opinion, which will come at the end of 2024 at the earliest, but more likely in 2025.

1. **Certification Process**

To take advantage of the Framework, testing organizations may pursue one of two options. Companies that were formerly certified under the Privacy Shield agreement are automatically included in the new Framework. These companies are required to update their privacy policies with the new details of the EU-US DPF by October 10, 2023. The privacy policy revisions must state the company’s commitment to follow the DPF.

Any other US company can certify its participation in the Framework by committing to comply with a detailed set of privacy obligations. This could include, for example, privacy principles such as purpose limitation, data minimization and data retention, as well as specific obligations concerning data security and the sharing of data with third parties.[[9]](#footnote-9)

Once these revisions have been completed, a company may rely immediately on the EU-US DPF to receive personal data transfers from the EU. Otherwise, the only alternative to continue EU-US data transfers is for an organization to employ either standard contractual clauses or binding corporate rules, which as described above have proven to be burdensome, especially for smaller organizations.

The Department of Commerce charges an application fee for organizations desiring to self-certify under the EU-US DPF. Once approved, the application must be resubmitted annually. The fee schedule for self-certification is expected to remain the same as it was under the former Privacy Shield and is scaled to company size based on revenue and dependent on the number of Frameworks (i.e., EU, UK, Swiss). The annual “single Framework" fee for companies with revenue under $5 million is $250; fees

for companies with revenue from $5-25 million is $650.[[10]](#footnote-10) The timeline for Department of Commerce approval under the EU-US will depend on the volume of applications received.

Companies that were not formerly certified under the Privacy Shield that wish to qualify under the EU-US DPF may begin the initial self-certification application process by visiting DataPrivacyFramework.gov which became active on July 17. These companies must provide information in the initial application, including about their privacy policies, practices regarding the transfer of data, and who is responsible for the transfer. A company cannot rely on the Framework until the application has been approved by the Department of Commerce. Once approved, the company’s name is added to a formal list of registered organizations.

Importantly, nonprofits are currently excluded from participation in the EU-US DPF. Companies which fall under the jurisdiction of US financial regulators are also ineligible for certification under the EU-US DPF.

The Federal Trade Commission (FTC) is responsible for enforcing US companies’ adherence to the EU-US DPF. The FTC has recently announced that it will consider an organization’s failure to adhere to its privacy policy as a legal misrepresentation under the Fair Trade Act and an unfair trade practice.

**CONCLUSION**

Testing organizations wishing to take advantage of a streamlined self-certification process for transferring personal data between the EU and US may now rely on the new EU-US DPF. In the near term, the EU-US DPF ends an extended period of legal uncertainty for companies that rely on freely transferring data between the EU and the US. In the longer term, however, until the CJEU rules whether this new Framework is sufficient to protect European’s privacy rights under the GDPR, US companies will face some uncertainty about whether the Framework will survive the legal challenge.

As in previous situations, we will monitor any developments under the Framework as well as the litigation challenging it.

1. If Swiss test takers are involved, there must be a separate data transfer determination made under the pending Swiss adequacy decision. No data transfer benefits will arise under framework until the Swiss data protection authorities issue an adequacy ruling for the US. [↑](#footnote-ref-1)
2. On June 4, 2021, the European Commission adopted **a set of standard contractual clauses** for the transfer of personal data to countries outside of the EEA. The **SCCs are a tool for data transfers (**i.e. to comply with the requirements of the GDPR for **transferring personal data to countries outside of the EEA)**. They contain specific data protection safeguards to ensure that personal data continues to benefit from a high level of protection when transferred outside the EEA. They can be used by data exporters, **without the need to obtain a prior authorization** (for the data transfer or the clauses used) from a data protection authority. By adhering to the SCCs, data importers contractually commit to abide by a set of data protection safeguards. The SCCs are available here:[Standard contractual clauses for international transfers](https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en). [↑](#footnote-ref-2)
3. Most notably, the Irish Data Protection Commission fined Meta Platforms Ireland 1.2 billion euros for the unlawful processing, including storage, in the U.S. of personal data of EU users. Despite Meta’s reliance on SCCs and additional data protection measures to supplement the SCCs, the reasoning for the enforcement action boiled down to Meta’s inability to compensate for the deficiencies in U.S. law that were the cause of concern in the CJEU Schrems II decision. This decision has sparked concern that, if a company as large and technically sophisticated as Meta is not sufficient for data transfers to the US, small and medium organizations will struggle to permissibly transfer data from the EU to the US if the Framework cannot be relied upon. [↑](#footnote-ref-3)
4. On December 14, 2022, ODNI released to the public the [Intelligence Community Directive 126: Implementation Procedures for the Signals Intelligence Redress Mechanism](https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf) pursuant to EO 14086. <https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf>. [↑](#footnote-ref-4)
5. 50 U.S.C. § 3029 (provides the duties of the Civil Liberties Protection Officer). [↑](#footnote-ref-5)
6. 28 C.F.R. 201. [↑](#footnote-ref-6)
7. A similar adequacy ruling will be necessary by the UK to enable data transfers from the UK to the US. Such a decision is expected later in 2023. [↑](#footnote-ref-7)
8. We do want to note that, while it is unlikely there will be changes in US surveillance laws, US surveillance and data acquisition has also sparked legislative initiatives consistent with the spirit of EO 14086, partially in response to the contents of the declassified Office of the Director of National Intelligence (ODNI) National Intelligence Report (<https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf>). On July 14, 2023, H.R. 4639 was introduced that aims to prevent law enforcement and intelligence agencies from obtaining subscriber or customer records in exchange for anything of value. [↑](#footnote-ref-8)
9. See [Self-Certification Information (dataprivacyframework.gov)](https://www.dataprivacyframework.gov/s/article/Self-Certification-Information-dpf). [↑](#footnote-ref-9)
10. Organization’s Annual Revenue:               A Single Framework   /   Both Frameworks

$0 to $5 million                                            $250   /   $375

Over $5 million to $25 million                     $650   /   $975

Over $25 million to $500 million               $1,000   /   $1,500

Over $500 million to $5 billion                   $2,500   /   $3,750

Over $5 billion                                                $3,250   /   $4,875: [↑](#footnote-ref-10)