EUROPEAN COMMISSION ADOPTS EU-US DATA PRIVACY FRAMEWORK

On 10th July 2023, an agreement between the European Commission (the "Commission") and the United States was completed to facilitate transfers of personal data from the European Economic Area (EEA) to the United States of America (US). The agreement, known as the EU-US Data Privacy Framework[1] (the "Framework"), follows a backdrop of uncertainty between the two jurisdictions which had arisen due to privacy concerns from an EU law perspective over the use and storage of personal data in the US.

1. Adequacy decision EU-US Data Privacy Framework_en.pdf (europa.eu)

"US organisations which adhere to the new Framework will be able lawfully to receive EEA personal data without any additional transfer mechanism."

Under the new Framework, self-certified US organisations will be able to process EU personal data, subject to a detailed set of privacy obligations which must be adhered to and new safeguards in the area of US government access to data. Among others, these obligations on US organisations include the deletion of personal data when no longer necessary for the purpose for which it was collected and continuity of protection when personal data is shared with third parties. In addition, the safeguards require that access to such data will only be shared with US public bodies and law enforcement agencies in particular for criminal law enforcement and national security purposes when it is "necessary and proportionate" in the interests of national security.

US organisations which adhere to the new Framework will be able lawfully to receive EEA personal data without any additional transfer mechanism. The Commission has stated that the Framework "adequately" addresses the concerns formerly raised by the Court of Justice of the European Union ("CJEU") concerning the security of transfers of personal data to the US, having regard to the access of US surveillance authorities.

After years of failed negotiations with the US, the Framework marks a significant development in establishing clear data protection measures for the transfer of personal data from the EEA to the US, and an important step by the Commission in providing confidence to EEA citizens that their data will be safe. But the Framework will only facilitate transfers of personal data from the EEA to US organisations which sign up to it.

Background – *Schrems II*

The significance of protecting the security of personal data transferred outside the EEA arose in the *Schrems II*[2] judgement, handed down by the CJEU on 16 July 2020 (further commentary on which can be found here)[3]. In this case, Chapter V of the EU General Data Protection Regulation (GDPR) was considered, which restricts the transfer of personal data internationally outside the EEA. The purpose of this is to ensure that personal data being transferred outside the EEA should still be protected to an equivalent standard to that under the GDPR. To comply with the GDPR, organisations must meet at least one of the following criteria:

1. The transfer of personal data is to a country which benefits from a decision of the Commission that the country ensures an adequate level of protection of personal data (Adequacy Decision);
2. One of the safeguards set out in Article 46 of the GDPR – which include use of the Commission's 'Standard Contractual Clauses' for international transfers ("SSCs") - applies to the transfer; or
3. One of the derogations set out in Article 49 of the GDPR applies to the transfer in occasional circumstances.

As a limited number of countries have been recognised by the Commission as benefitting from an Adequacy Decision, organisations have predominantly relied on safeguards to justify their transfer of personal data. Use of the SSCs are often the most practical way in which organisations can lawfully transfer personal data outside of the EEA (or the UK as parallel provisions apply under the UK GDPR).

In *Schrems II*, data protection activist Max Schrems complained to the Irish Data Protection Commissioner about the transfer of his personal data by Facebook from Ireland to the United States. This led to the CJEU judgement in *Schrems I*[4] which determined the invalidity of the 'Safe Harbour' framework, which had previously facilitated the transfer of personal data from

2. *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18.*
3. **https://www.hfw.com/International-data-transfers-from-the-EEA-and-UK-Take-care-July-2020**
4. Maximillian Schrems v Data Protection Commissioner, Case 362/14. See our briefing on *Schrems I* **here**

the EEA to US organisations which had signed up to adhere to the 'Safe Harbour'. Following this, the 'Safe Harbour' was replaced by the 'Privacy Shield', which allowed personal data to be transferred from the EEA to US organisations which had signed up to it.

In *Schrems II*, the CJEU questioned both the validity of using the Privacy Shield to transfer personal data to the US and the validity of using SCCs to transfer personal data to the US. It was held that the Privacy Shield was inadequate for complying with the GDPR due to the disproportionate level of access US surveillance authorities had to personal data. Moreover, the judgement emphasised that EEA Member States had the power to suspend or restrict transfers of personal data to third countries if an adequate level of protection could not be guaranteed, regardless of whether or not SCCs were used.

The CJEU held that the use of SCCs alone was not prohibited, however their use in isolation was not sufficient for GDPR purposes. SCCs are a valid mechanism for international transfers under Article 46 of the GDPR, provided that additional assessments are undertaken by the organisation relying on them. The assessments must consider the level of protection for transfers and ensure that individuals, ie data subjects, are afforded appropriate safeguards and enforceable rights. The assessments should be made on a case-by-case basis and consider the laws of the country in which the recipient organisation is located and consider a range of assessment factors set out in Article 45(2) of the GDPR. These include respect for human rights, access by public authorities to personal data, and redress avenues afforded to data subjects. Organisations may be required to supplement the SCCs with additional safeguards if deemed necessary.

The result of *Schrems II* was a significant degree of legal uncertainty regarding the transfer of personal data to countries outside the EEA (or UK).

The Framework

In its adequacy decision, the Commission sets out that the Framework is based on a system of self-certification by which US organisations commit to a set of privacy principles – the 'EU-US Data Privacy Framework Principles' including the Supplemental Principles (together, the "Principles"). These Principles are intended to provide data subjects with clarity on how their personal data is processed, as well as ensuring accountability for the US organisations handling the personal data.

US organisations wishing to be self-certified must first be subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) or the U.S. Department of Transportation (DoT) in order to be deemed eligible. After self-certification, an organisation is immediately subject to the Principles of the Framework.

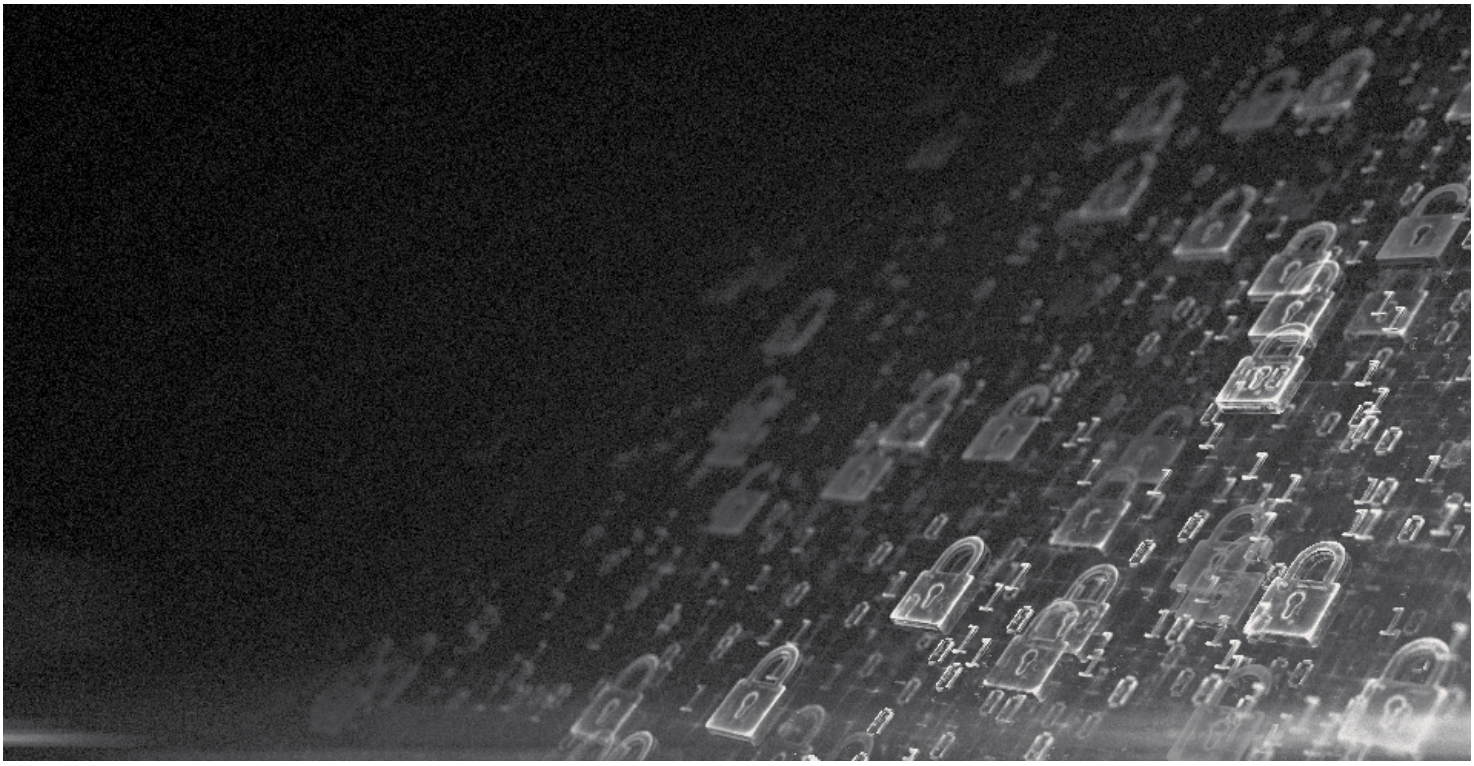
The key Principles of the Framework are as follows:

1. Purpose limitation and choice

   Personal data should be processed "lawfully and fairly" and limited only to the specific purpose indicated to the data subject. For any similar but new purposes for using the personal data, the organisation must provide data subjects with the opportunity to opt out via a clear and readily available mechanism.

2. Processing of special categories of personal data

   Specific safeguards are applied to categories of personal data where "sensitive information" is involved such as medical, political, religious, or racial information. Any data which is considered sensitive



under the GDPR[5] (defined in the GDPR as Special Categories of personal data) will equally be considered as sensitive under the Framework by self-certified US organisations.

3. Data accuracy, minimisation, and security

   Data held by US organisations should be accurate and relevant, and processing must not exceed its intended purpose as well as only being held for the necessary duration to satisfy the intended purposes of processing. If necessary, organisations should also take steps to ensure that the personal data is kept up to date. To ensure security, personal data should only be kept in a manner which makes the data subject identifiable for as long as it serves the purpose for which it was initially collected. Organisations must also take steps to ensure the secure storage and protection of such information, as required by Article 32 of the GDPR.

4. Transparency

   Data subjects should be afforded full transparency over the use and handling of their personal data. This may include transparency over the type of data being collected, its purpose, the type or identity of third parties who may access it, and available redress avenues (among others). Organisations must maintain their privacy policies to ensure that they comply with the Principles and ensure that these policies are made public.

5. Individual rights

   US organisations are subject to various rights which data subjects can enforce against them, such as the right to request access to personal data and the right to object to the processing of personal data. Organisations are required to respond to such requests from data subjects within a "reasonable" timeframe.

6. Restrictions on onward transfers

   The protection given to data being transferred from the EEA to the US must not be compromised by any further transfers from the US to a third county. Special rules apply to such "onward transfers" including the rule that any onward transfer can only take place for limited and specific purposes and only if the level of protection given by the recipient will be no less than the level set out in the Principles.

7. Accountability

   To ensure their compliance with the Principles, US organisations are required to establish clear and effective measures on the handling of personal data. They must have a mechanism in place to demonstrate such compliance to the competent supervisory authority through, for example, a thorough self-assessment or external compliance review process such as an audit. US organisations must also retain records on the implementation of their data protection practices which must be readily available for review.

Supplemental Principles

Aside from the key Principles, self-certified US organisations must comply with the Supplemental Principles which expand on the main set of Principles and are equally binding on them.

The Supplemental Principles are categorised as follows:

- Sensitive Data
- Journalistic Expectations
- Secondary Liability
- Performing Due Diligence and Conducting Audits
- The Role of the Data Protection Authorities

5. **CL2016R0679EN0000020.0001.3bi_cp 1..1 (europa.eu)**

"The data bridge will form part of the broader "Atlantic Declaration" agreed between President Biden and Prime Minister Sunak."

- Self-Certification
- Verification
- Access
- Human Resources Data
- Obligatory Contracts for Onward Transfers
- Dispute Resolution and Enforcement
- Choice – Timing of Opt-Out
- Pharmaceutical and Medical Products
- Public Record and Publicly Available Information
- Access Requests by Public Authorities

Self-certified organisations are also required to re-certify their adherence to the Principles annually to ensure continuous compliance with the Framework.

EEA data subjects will benefit from several redress avenues in case their data is wrongly handled by US organisations. This includes free of charge independent dispute resolution mechanisms and an arbitration panel.

In addition, as part of the Framework, data subjects in the EEA will have access to an independent redress mechanism regarding the collection and use of their data by US intelligence agencies. This will include the new Data Protection Review Court (DPRC) which will independently investigate and resolve complaints, including by adopting binding remedial measures. If the DPRC finds that data was collected in violation of the new safeguards, it will be able to order the deletion of the data.

Next Steps

The adoption of the Framework presents a significant opportunity for the US and EU to boost their economic relations, with transatlantic data flows between the US and EU estimated to be valued at over $7.1 trillion dollars[6].

The Framework has not been immune to criticism, however. Max Schrems has, among others, threatened legal action against the Framework on the basis that it was "*not based on material changes but by political interests*[7]". Schrems is expected to bring a new legal challenge in the CJEU by the end of the year, citing the Framework as a failure in resolving core issues and campaigning for changes in US surveillance laws to make any regulations tenable. Schrems is calling on the CJEU to suspend the deal in the interim.

Aside from this, the implementation of the Framework will be subject to periodic reviews to ensure its effectiveness and it is anticipated that the first review will take place within one year of the Commission's adequacy decision's entry into force.

The UK continues to govern data protection via the UK GDPR and Data Protection Act 2018. However, the UK government is working towards its own adequacy framework for transfers of personal data from the UK to the US after announcing in June 2023 that both the UK and US have committed to establishing a "data bridge[8]". This would act as an extension of the EU-US Framework and has been dubbed the "Privacy Shield 2.0". The US-UK data bridge would constitute a UK-issued adequacy decision when finalised and would avoid the need for UK business to use inefficient transfer mechanisms when transferring personal data to the US. The UK government intends to consult the Information Commissioner's Office (ICO) on the UK-US data bridge in the coming months. The data bridge will form part of the broader "Atlantic Declaration" agreed between President Biden and Prime Minister Sunak which includes a commitment to ensuring responsible development of technological and trade relations including data protection and artificial intelligence.

It is likely that the UK will adopt similar safeguards as set out in the EU-US Framework. However, in the meantime, UK businesses must continue to use alternative mechanisms recognised by the UK GDPR to ensure lawful transfers of personal data from the UK to the US, such as continued use of the ICO's International Data Transfer Addendum to the European Commission's SCCs or of the ICO's International data transfer agreement.

For further information, please contact.

ANTHONY WOOLICH
Partner, London,
T +44 (0)20 7264 8033
E anthony.woolich@hfw.com

Assistance provided by Lucy Macris, Trainee Solicitor.

6. **FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework | The White House**
7. **European Commission gives EU-US data transfers third round at CJEU (noyb.eu)**
8. **Joint statement on the UK-US data bridge - GOV.UK (www.gov.uk)**

HFW has over 600 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our EU, Competition and Regulatory capabilities, please visit hfw.com/EU-Competition-and-Regulatory.

Americas | Europe | Middle East | Asia Pacific