Katten

PRIVACY, DATA AND CYBERSECURITY ADVISORY

Key Principles and Considerations for Participation in the EU-US Data Privacy Framework

July 25, 2023

This note summarises and highlights the key aspects of the EU-US Data Privacy Framework following the European Commission's adequacy decision on July 10. The contents of this note are general in nature. Specific advice should be taken in particular circumstances.

Overview: The EU-US Data Privacy Framework

On July 10, the European Commission adopted its long-awaited adequacy decision for the EU-US Data Privacy Framework (EU-US DPF). The adequacy finding means personal data can now be transferred from EU entities to US entities that have obtained the EU-US DPF certification, subject to certain requirements. This is welcome news, as such certified entities will no longer need to rely on additional safeguards such as the EU Standard Contractual Clauses (EU SCCs) to do so. However, the EU-US DPF may not suit all business models, so a careful assessment should be made of whether compliance with the framework is achievable and cost-effective. Read on to find out more.

The EU-US DPF Principles

The requirements under the EU-US DPF are principle-based, which align with the General Data Protection Regulation (EU) 2016/679 (GDPR). The aim is to ensure individuals located in the EU continue to benefit from the protections imposed by the GDPR when their personal data is transferred to the US.

The US Department of Commerce (DoC) will only certify US organisations that commit to adhering to the seven key principles as well as the supplementary principles (Principles).

1. The Notice Principle – transparency on data processing arrangements.
2. The Choice Principle – the choice for individuals to stop their personal data from being disclosed to a third party or used for a purpose different from the purpose(s) for which it was originally collected.
3. The Accountability for Onward Transfer Principle – accepting responsibility for onward transfers.
4. The Security Principle – ensure data is secure.
5. The Data Integrity and Purpose Limitation Principle – data must be accurate, complete, current, and limited to what is relevant for processing.
6. The Access Principle – individuals have rights of access, amendment, rectification and deletion of personal data.
7. The Recourse, Enforcement and Liability Principle – enable effective legal protection and recourse for individuals.

Certification

To participate in the EU-US DPF, organisations must publicly declare their commitment to compliance with the Principles. As part of this public declaration, privacy policies must be publically available and the applying entity must provide information to the DoC on its processing activities. Behind closed doors, organisations will also need to keep paper trails demonstrating their compliance with the Principles.

A key aspect for organisations considering the certification are the costs. Annual fees are payable and tiered based on an organisation's annual revenue. Fees range from $250 to $4,875. There will also likely be additional costs for legal fees to ensure all information and documents provided to the DoC are accurate and sufficient, in addition to fees for advice on implementing the independent recourse mechanism as required.

Enforcement

While joining the EU-US DPF is voluntary, once an organisation self-certifies and publicly declares its commitment to adhering to the Principles, that commitment becomes enforceable under US law. Organisations should therefore be mindful of the point at which they sign up and become liable to enforcement action under US law.

The Federal Trade Commission (FTC) and the Department of Transportation (DOT), the governing bodies under the EU-US DPF, have stressed their commitment to enforcement through the implementation of compliance orders or financial penalties for continuing violations.

Any persistent failures to comply with the Principles will result in removal from the DPF List, and the organisation must return or remove all personal data received under the EU-US DPF.

Practical Implications

Whether participation in the EU-US DPF is right for an organisation will require a targeted analysis of its operations to identify whether this will be commercially beneficial. Organisations considering the certification should contact a data privacy lawyer to help them identify whether the EU-US DPF is suitable in contrast to the tried and tested use of EU SCCs.

For organisations deliberating what participation in the EU-US DPF may mean for them practically, we have outlined some key considerations:

- Do you have the means to put in place continuous compliance, monitoring and verification methods? These will be required to ensure your organisation is operating in accordance with the Principles and your privacy policy.
- How will you ensure you have an effective complaints process? Is there someone you can select internally as a point of contact to handle complaints or will you need a third party resource?
- Could you appoint a designated EU-US DPF Compliance Officer? This role could involve assisting with the handling of certification and re-certification of the organisation, along with being responsible for updates to policies and verification procedures.
- Do you have the means to maintain records of your compliance in the event that there is an investigation or complaint from a data subject or enforcement authority?
- Do the potential costs (both in time and money) make commercial sense for your organisation when evaluated against your data flows?

For help with assessing these implications, any other key considerations and the certification process itself, don't hesitate to contact us using the details below.

CONTACTS

For more information, please contact your Katten lawyer or any of the following Intellectual Property lawyers.

Sarah Simpson
+44 (0) 20 7770 5238
sarah.simpson@katten.co.uk

Tegan Miller-McCormack
+44 (0) 20 7770 5247
tegan.miller-mccormack@katten.co.uk

Brigitte Weaver
+44 (0) 20 7770 5235
brigitte.weaver@katten.co.uk

**Hayley Rabet, a trainee in the Intellectual Property practice, contributed to this advisory.*