Department for Science, Innovation & Technology

Factsheet for UK Organisations

Headlines

From **12 October 2023,** businesses in the UK can start to transfer personal data to US organisations certified to the "UK Extension to the EU-US Data Privacy Framework" (UK Extension) under Article 45 of the UK GDPR without the need for further safeguards such as those set out in Articles 46 and 49 of the UK GDPR. UK organisations should be mindful of the need to update privacy policies and document their own processing activities as necessary to reflect any changes in how they transfer personal data to the US.

The EU-US Data Privacy Framework (DPF) is a bespoke, opt-in certification scheme for US organisations, enforced by the Federal Trade Commission (FTC) and Department of Transportation (DoT), and administered by the Department of Commerce (DoC).

The Data Privacy Framework includes a set of enforceable principles and requirements that must be certified to, and complied with, in order for organisations to be able to join the Data Privacy Framework. These principles take the form of commitments to data protection and govern how an organisation uses, collects and discloses personal data.

US organisations who have been certified to the Data Privacy Framework can opt in to receiving data from the UK.

Once a US organisation has been certified and is publicly placed onto the Data Privacy Framework List (DPF List) on the DPF website they can receive UK personal data through a UK-US data bridge.

What types of organisations are included and excluded under the DPF?

UK organisations cannot simply transfer personal data to any data importer/recipient in the US - for the data to flow freely, the relevant recipient must be certified to the UK Extension and appear on the DPF List.

Only US organisations subject to the jurisdiction of the US FTC or the US DoT are currently eligible to participate in the DPF program. Those US organisations not subject to the jurisdiction of either the FTC or DoT — for example, banking, insurance, and telecommunications companies — are unable to participate in the DPF program at this time.

What categories of data are excluded from transfer under the DPF?

Journalistic data defined by Supplemental Principle 2(b) of the EU-US Data Privacy Framework is not subject to the requirements of the EU-US DPF. Therefore, such data **cannot** be transferred under the UK-US data bridge.

For information, the Journalistic Exceptions Supplemental Principle 2(b):

> *Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Principles.*

Should special category or sensitive data be shared under the UK-US data bridge?

The Choice principle under the DPF does not mirror exactly the definition of special category data in Article 9(1) UK GDPR, as it does not include genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning sexual orientation. However, this is mitigated by the fact that the choice principle specifies that organisations under the DPF are also required to treat as sensitive any information received which is identified and treated as sensitive by third parties sharing the information.

Special category and sensitive data can be shared with US organisations under the DPF, **however** this must correctly be identified by UK organisations as such when it is being shared.

The Choice principle 2(c) sets out that:

> *personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual*

are considered sensitive information under the DPF. US Organisations under the DPF are also required to treat as sensitive any information received which has been identified and previously been treated as sensitive by the organisation sharing the information.

For UK personal data which is considered to be sensitive, and which is not covered by the list set out within the Choice principle, it must be appropriately **identified** as sensitive to US organisations when transferred under the UK-US data bridge to ensure it receives appropriate protections under the DPF. This will include:

- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- data concerning sexual orientation

Should criminal offence data be shared under the UK-US data bridge?

Where criminal offence data is proposed to be shared under the UK-US data bridge as part of a human resources (HR) data relationship, US recipient organisations are required to indicate that they are seeking to receive such data under the DPF.

HR data is clarified under Human Resources Data Supplemental principle 9(a)(i) as:

> *…personal information about its employees (past or present) collected in the context of the employment relationship [transferred] to a parent, affiliate, or unaffiliated service provider in the United States participating in the EU-U.S. DPF…*

Criminal offence data may also be shared outside of a HR relationship.

When sharing Criminal offence data it should be indicated to the US recipient organisation that it is sensitive data requiring additional protections, in line with protections for special category or sensitive data set out in the question above.

The Information Commissioner's Office website contains additional information relating to "what is criminal offence data": https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/criminal-offence-data/what-is-criminal-offence-data/

How can you check which specific businesses have certified to the UK Extension?

Before sending personal data to the US, you must confirm that the recipient is certified with the DPF (and when transferring HR data specifically, US organisations must have highlighted this on their certification). More precisely, you must:

1. Confirm whether an organisation is an active DPF participant, go to the DPF List[1] and search alphabetically or by typing in the organisation name in the search bar..

2. Confirm that said organisation has signed up to the UK Extension to the EU-US Data Privacy Framework program.

3. (if wishing to transfer HR data) Confirm that HR data is covered by the organisation's DPF commitments:

- Click on the organisation's name within the DPF List.[2]
- Within the organisation's DPF program record, click on the link to the relevant privacy policy or policies (for HR data and/or non-HR data) under the "Privacy Policy" section of the record.

4. Review the privacy policy that applies to the covered information:

- Within the organisation's DPF program record, click on the link to the relevant privacy policy or policies (for HR data and/or non-HR data) under the "Privacy Policy" section of the record.

If you cannot rely on the UK Extension to transfer personal data to the US, your organisation will have to revert to one of the pre-existing appropriate safeguards (e.g., the International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses) or rely on one of the available derogations under Article 49 of the UK GDPR for international data transfers. You may also need to carry out a transfer risk assessment[3] to validate your transfers.

1. https://www.dataprivacyframework.gov/s/participant-search
2. https://www.dataprivacyframework.gov/s/participant-search
3. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/international-data-transfer-agreement-and-guidance/transfer-risk-assessments/