Data Protection update – October 2023

There has been a significant development in the rules relating to transfers of personal data to the US, so today's update covers those changes as well as serving as a useful reminder of your other responsibilities and obligations in relation to data protection.

Transfers to US companies under the Data Privacy Framework (DPF)

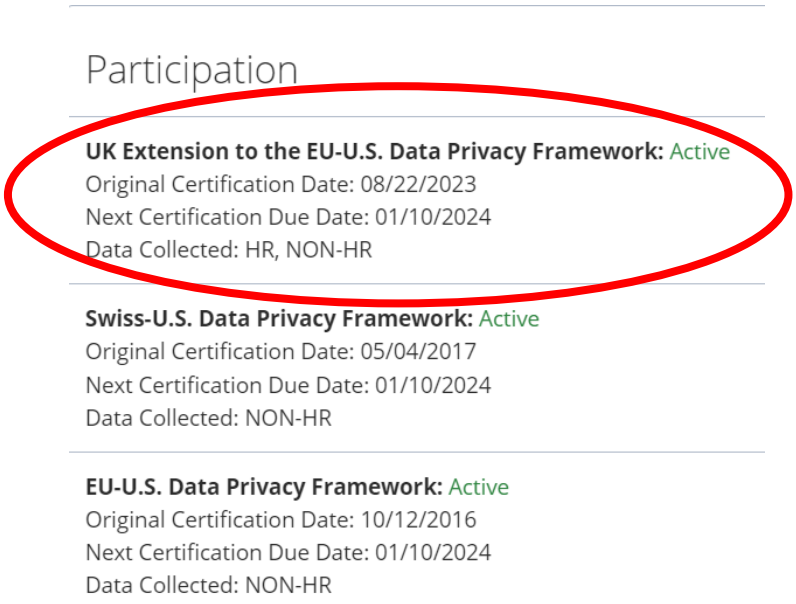
If you need to transfer personal data to a US-based company for any reason, that company **might** be covered under the Data Privacy Framework.

This is a new initiative, originally agreed between the US and the EU, whereby US companies can self-certify their compliance with rules and regulations relating to data protection and privacy which offer a similar level of protection as the EU (and UK) GDPR. Since 12th October 2023, this initiative has been extended to the UK under the "UK Extension to the EU-US Data Privacy Framework".

Once a US company is certified under the UK Extension, you can make the transfer of personal data to that company without further restrictions, other than notifying affected data subjects that their personal data will be or might be transferred overseas.

Before making any transfer, you should check if the receiver is certified under the DPF (you can search for companies using this link). The receiver must be certified specifically for the UK Extension.

This is what the receiving company's entry should look like on the DPF website:



Do make sure that if you're sharing any special categories of data (also known as "sensitive" personal data), you make the receiver aware of this before you make the transfer. You might

find it helpful to draft a list of the types of personal data you hold (and might share with other companies), and which of those you consider to be sensitive personal data. You can then share that list with any companies you are making data transfers to under this new DPF arrangement.

For more information, please see this factsheet, or the gov.uk website.

International data transfers (general rules and principles)

Data transfers to organisations outside the UK are restricted. A transfer is defined as "sending or making available personal data to another business or organisation" which is based outside the UK.

Transfers to employees of the same company but based in different countries is not restricted, but transfers between companies (or employees of those companies) in the same group is restricted because they are different legal entities. Transfers from one processor in the UK to another processor in the UK that is electronically routed via another country are unrestricted.

All other types of data transfer are restricted and transfers can only be made in one of the following circumstances (and reasons for transfers must be considered in this order):

I. **The country you are transferring to has an "adequacy regulation" in place**. The current list is as follows: all EEA countries, Gibraltar, Korea, Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay, Japan (but only if the transfer is to a company who is subject to Japan's Act on the Protection of Personal Information) and Canada (only for personal data which is covered by the Personal Information Protection and Electronic Documents Act (PIPEDA)).

II. The recipient company is a US-based company which is listed on the DPF website and has an **active UK Extension certification in place**.

III. **The transfer is covered by appropriate safeguards**. The list of possible safeguards is below; however please note that just having these safeguards in place is not sufficient in itself, you must also **conduct a Transfer Risk Assessment (TRA)** to determine if the safeguards are really sufficient, taking account of (a) the protections contained in the mechanism you're using to make the transfer and (b) the legal framework of the destination country (including laws governing public authority access to the data). The ICO has further guidance on TRAs here.

    These are the accepted methods for transfers under the appropriate safeguards mechanism:

    - **Standard contractual clauses.** This is the most likely option you will use and is explained in more detail below.
    - Binding corporate rules which have been approved by the ICO (intended for multinational corporate groups). A list of the companies who have approved BCRs in place is available here.
    - Code of conduct that has been approved by the ICO (none have been approved as yet).

- Certification scheme approved by the ICO (none have been approved as yet).
- Legally binding instrument between public authorities (not likely to be applicable to your business).
- Administrative arrangements between public bodies (not likely to be applicable to your business).

IV. **The transfer is covered by an exception**. Exceptions are to be used sparingly, not as a general rule for data transfers. They can only be used where there is no adequacy regulation and you cannot use any of the "appropriate safeguards" options. There are 8 exceptions, but I have included only those that are applicable to private companies.
- **Explicit consent from the data subject.** This is the most likely option you will use and is explained in more detail below.
- To make or defend a legal claim.
- You have a contract with the data subject that actively requires you to transfer their personal data outside the UK in order to enter into or comply with the contract. This option can only be used for occasional transfers and is not suitable for regular transfers.
- You have compelling legitimate interests. This option can only be used as a "one-off", is for truly exceptional circumstances, and must be notified to the ICO and the affected data subjects.

1. Standard contractual clauses (SCCs)

The ICO has drafted template contracts to be used between data exporters and data importers. The templates are here. You must use the ICO SCCs for any new contracts you enter which require any transfer of personal data. You must also use the ICO SCCs for any contracts that originally used the EU SCCs if those contracts continue past 21st March 2024.

Please be aware the ICO SCCs cannot be incorporated via hyperlinks into contracts. The Data Transfer Agreement must be filled out for each client or supplier to whom you transfer data internationally, and must be signed as a separate document in addition to your terms and conditions.

2. Explicit consent for international data transfers.

If you choose to use the exception of "explicit consent" for the transfer of data internationally, you must follow the following conditions.
- The consent given must be specific and informed, and you must provide the data subject with precise details of the transfer (you cannot use an overarching or general consent mechanism).
- You must tell the data subject:
  - the identity of the receiver, or the categories of receiver;
  - the country or countries to which the data is to be transferred;
  - why you need to make a restricted transfer;
  - the type of data being transferred;
  - the data subject's right to withdraw consent; and
  - the possible risks involved in making a transfer to a country which does not provide adequate protection for personal data and without any other appropriate safeguards in place.

- If the data subject withdraws his or her consent at any point, you cannot transfer the personal data internationally from that date onwards. For this reason, using consent as a mechanism for data transfers is not recommended except in occasional circumstances.

Other general obligations under data protection laws

I. **The seven key principles**
You must ensure that you're complying with each of the key principles of the UK GDPR. That includes regular assessments of whether your security arrangements are sufficient and suitable; ensuring your privacy notices and/or policies are comprehensive and cover all your processing activities; and that you have a suitable legal basis for all the processing activities you (or the data processors you appoint) undertake. More information is available here.

II. **Contracts between data controllers and data processors**
Contracts between data controllers and their processors must contain certain mandatory clauses. Please ensure that all your contracts are compliant with these requirements.

III. **Processing activities**
You are required by law to maintain records of all your processing activities. Now is a good time to review those records to ensure they are still adequate and relevant. As part of your processing activities, you are required to conduct DPIAs (data protection impact assessments) on any new projects, systems, software or other methods of processing personal data that are likely to result in high risk to individuals' interests. The ICO has a DPIA template that you can use here.

IV. **Direct marketing**
Marketing activities via electronic means (phone, fax, email or text) and cookie monitoring is governed by PECR (Privacy and Electronic Communications Regulations). The ICO has more information and guidance on PECR here.

If you need any additional information, or require help and support with any of the above, please contact bernie@labvolution.com.