Mackrell Turner Garrett

International Data Transfers

A Quick Guide

This guide is intended to give an overview of the requirements for the transfer of personal data by data controllers in the UK to countries outside the European Economic Area ("**EEA**") as prescribed by the Data Protection Act 1998 ("**the Act**") and European Community Directive 95/46/EC ("**the Directive**").

There are eight data protection principles in the Act which are often referred to as the principles of "good information handling". The eighth principle of the Act states that:

"Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data".

Compliance with the eighth data protection principle can in most cases be reached by way of a four step test as detailed overleaf.

Mackrell Turner Garrett

STEP 1 – TRANSFER OR TRANSIT?

Is the data to be processed being transferred outside the EEA, or is it merely in transit through a third country to another EEA country?

The transfer of data, given that the term "transfer" is not defined in the Act, is the transmission from one place or person to another. This means if data simply passes through a third country on its way from the UK to another country in the EEA, it will not be caught by the eighth data protection principle.

STEP 2 – DOES THE THIRD COUNTRY PROVIDE ADEQUATE LEVELS OF PROTECTION?

Once it has been determined that there will be a transfer of personal data to a third country, the data controller must be satisfied that the personal data will be adequately protected in that third country.

Community findings of adequacy – The European Commission ("**Commission**") has stated that there are currently seven countries outside the EEA which provide adequate levels of protection for personal data, which include Switzerland, Canada and Argentina. If personal data is being transferred to any of these countries the transfer will comply with the eighth data protection principle of the Act.

Safe harbor scheme – This scheme consists of certain principles which are similar to those contained in the Act and allows US organisations in certain sectors to state that they will adhere to the principles of the scheme. If data is being transferred to a US organisation which has certified that they will adhere to the principles of the scheme, the transfer to that US organisation will comply with the eighth data protection principle.

Assessment of adequacy – Where the data protection laws of a third country have not been subject to a Commission finding of adequacy, it is possible for the exporting controller of the data to assess the data protection regime in that country to see if it complies with the Act and the Directive.

The exporting controller must consider the "general adequacy criteria" such as the nature of the data, the purpose for which the data will be used and any other risks involved in the transfer. "Legal adequacy criteria" must also be assessed including the law in force in that country and any relevant codes of conduct. It may be appropriate for the exporting controller to seek local legal advice to assess how the national data protection laws compare to the protections afforded under the Directive and the Act.

If the exporting controller is satisfied with the protection that the third country will offer then the transfer will comply with the eighth data protection principle.

STEP 3 – CAN THE PARTIES IMPLEMENT ADEQUATE SAFEGUARDS TO PROTECT THE DATA?

If the exporting data controller cannot establish adequacy in the third country, the parties to the data transfer can implement adequate safeguards by one of the following means:

Model Clauses – Certain Commission authorised model clauses can be inserted into a contract between the exporting data controller and the importing party in the third country.

Binding Corporate Rules ("**BCRs**") – Multinational companies can create BCRs to implement adequate data protection safeguards. These BCRs must first be approved by the Information Commissioner which will ensure that transfers from the UK may be made within the company's group.

If either the Commission approved model clauses or BCRs are implemented, the data transfer will comply with the eighth data protection principle.

STEP 4 – EXCEPTIONS TO THE EIGHTH DATA PROTECTION PRINCIPLE

Should it not be possible to comply with any of the above steps, it may be possible to rely on a number of exceptions to the eighth data protection principle, which include:

- Consent of the data subject.
- Necessity of transfer of data to comply with a contract between the transferor and the transferee.
- The transfer is in the benefit of the public interest.
- The transfer is necessary for legal proceedings.
- The transfer is in the vital interest of the data subject.

Compliance with the Directive is vital for any EEA-based entity. Whilst the above steps show how the transfer of personal data to a third country can be achieved in most circumstances, the data controller should always consider whether it is possible to achieve the organisation's goal without transferring the data outside the EEA so as to best protect the data subjects and their rights.

If you would like to talk about your legal obligations regarding any issues raised within this guide please contact Maung Aye on **00 44 (0) 20 7240 0521** or **Maung.Aye@mackrell.com**