Please note: The following information has not been updated since the Data Protection Act 2018 became law. Although there may be some subtle differences between the guidance in this document and guidance reflecting the new law – we still consider the information useful to those in the media. This guidance will be updated soon to reflect the changes.

Assessing Adequacy

International data transfers

Data Protection Act

The Data Protection Act 1998 (DPA) is based around eight principles of 'good information handling'. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

An overview of the main provisions of DPA can be found in The Guide to Data Protection. This is part of a series of guidance, which goes into more detail than the Guide to DPA, to help you to fully understand your obligations, as well as promoting good practice.

This guidance explains how a data controller should carry out an assessment of the adequacy of the protection available in respect of his proposed transfer of personal data outside the EEA.

Overview

A data controller may only transfer personal data outside the EEA to a country whose data protection laws have not been approved by the European Commission as providing adequate protection for data subjects' rights if there is an adequate level of protection for the rights of data subjects.

The adequacy of the level of protection associated with a particular transfer may be ensured in a number of ways. The data controller may:

- carry out his own assessment of the adequacy of the protection;
- use contracts to ensure adequacy;
- obtain Commission approval for a set of Binding Corporate Rules governing intra-group data transfers; or
- rely on one of the exceptions to the prohibitions on transfers of personal data outside the EEA.

This guidance considers how a data controller may carry out his own assessment of the adequacy of the protection available in respect of

a particular proposed transfer of personal data outside the EEA.

What the DPA says

The eighth data protection principle provides 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"
>
> (Part 1 of Schedule 1 to the DPA).

If you decide you need to transfer personal data outside the EEA, and the recipient is not in a country subject to a positive finding of adequacy by the Commission, nor signed up to the EU-US Privacy Shield, you will need to:

- conduct a risk assessment into whether the proposed transfer will provide an adequate level of protection for the rights of the data subjects; or
- if you do not find there is an adequate level of protection, put in place adequate safeguards to protect the rights of the data subjects, possibly using Model Contract Clauses or Binding Corporate Rules; or
- consider using one of the other statutory exceptions to the Eighth Principle restriction on international transfers of personal data.

This paper provides advice on the first of these options - assessing whether there is an adequate level of protection for a proposed transfer of personal data.

Adequacy criteria

The Data Protection Act (Schedule 1, Part II paragraph 13) provides that, when considering whether there is 'an adequate level of protection' for the purposes of the eighth principle, the level of protection must be one which is "adequate in all the circumstances of the case". In addition, in assessing adequacy, particular consideration should be given to specific listed criteria. For ease of reference these criteria may be divided into two groups; 'general adequacy criteria' and 'legal adequacy criteria'.

If an assessment of the 'general adequacy criteria' has revealed that, in the particular circumstances of the case, the risk to the rights of data subjects associated with the transfer is low, an exhaustive analysis of the 'legal adequacy criteria' may not be necessary. If a high risk is identified (e.g. if the data is particularly sensitive) then a more comprehensive investigation of the legal adequacy criteria will be required.

General adequacy criteria

- The nature of the personal data

  The transfer of some types of personal data will pose little risk to the rights and freedoms of individuals (e.g. the transfer of a list of internal telephone extensions to overseas subsidiaries of a multinational company would not be considered to be high risk as it is unlikely that a data subject would suffer significant damage if his business telephone number was obtained by an unauthorised recipient). Conversely, if a data exporting controller is proposing a transfer of sensitive personal data (e.g. health records) the level of protection required for the data (and the rights of the data subjects) will clearly be higher.

- The purposes for which the data are intended to be processed

  Some purposes for which data are processed will carry greater risks to the rights of the individuals than others. For example, if the data are to be processed for internal company or group purposes only (such as the internal company telephone list as described above) the transfer of such data may involve less risk to the rights of the data subjects than if the data transferred is to be distributed more widely (e.g. customer contact details to be used in marketing or on an internet site).

- The period during which the data are intended to be processed

  If the data are only to be processed once or for a short period of time and then destroyed, the risks arising from any lack of protection for data subjects' rights may be less than if the data are to be processed on a long-term basis. However, that is not to say that one-off transfers may be carried out without putting appropriate protection in place. It merely means that the data protection arrangements (such as regular reporting on security arrangements or security audits) may be less onerous n relation to such transfers or indeed may not be required at all.

- The country or territory of origin of the information contained in the data

  Consideration must be given to the country or territory from which the information originates (note that this is not necessarily the same as the country or territory from which the data is to be transferred). Where information has been obtained in a third country (i.e. outside the EEA) this will be a relevant factor as the data subjects may have different expectations as to the level of protection that will be afforded to their data than if the information been obtained in the EEA.

  Where the country (or territory) of origin of the information is outside the EEA it is important to remember that the DPA is not intended to provide a different level of protection for the data subjects rights than that provided by the data protection regime, if any, in the non-EEA country of origin.

- The country or territory of final destination of the information

  Transfers may be made in several stages involving transfers to one, then another, and then another country. Where it is known that there will be a further transfer to another country or territory, the level of protection given in the country of final destination will be relevant in assessing the adequacy of the protection associated with the transfer.

- Any security measures taken in respect of the data in the country or territory of destination

  Organisations exporting data may be able to ensure that the personal data are protected by means of technical measures (such as encryption or the adoption of information security management practices such as those in ISO27001/ISO27002. In practice, security is often a key factor in the commercial considerations of the parties.

Legal adequacy criteria

It will not always be necessary to carry out a detailed consideration of the legal adequacy criteria where consideration of the general adequacy criteria indicates that the risk to the rights of data subjects associated with the proposed data transfer is low. Where consideration of the general adequacy criteria indicates a higher risk, the legal adequacy criteria come into play. For example, where the exporting data controller is proposing to set up a permanent

operation in a third country and anticipates making regular, large-scale transfers to that country.

To make a legal adequacy assessment, consider the following:

- The law in force in the country or territory in question

  Consider whether the third country:

  - Has a data protection regime in place which meets the standards set out in the Article 29 Working Party document adopted on 24 July 1998 (WP 12).

  - Has any legal framework for the protection of the rights and freedoms of individuals generally.

  - Recognises the general rule of law and, in particular, the ability of parties to contract and bind themselves under contracts.

- The international obligations of the recipient country or territory

  Consider whether the third country has:

  - Adopted the OECD Guidelines[1] and put in place appropriate measures to implement the Guidelines.

  - Ratified Convention 108[2] and established appropriate mechanisms for compliance with the Convention.

- The rules or codes of practice which govern the processing of personal data in the third country.

  Consider whether the recipient country has in place any relevant codes of conduct or other rules (general or sectoral) enforceable in that country or territory (whether generally or by special arrangement in particular cases).

[1] 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' – Organisation for Economic Co-operation and Development, 1980
[2] Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data, Strasbourg 1981

Can the transfer proceed?

If adequacy is established further to your adequacy assessment, then the transfer can proceed from the UK to the third country in compliance with the eighth principle.

If transfers are taking place from more than one European jurisdiction then local advice should always be sought as there may be different requirements which apply depending on the jurisdictions in question.

If adequacy cannot be established it may be possible to put in place adequate safeguards or use one of the other exceptions to the Eighth Principle as discussed in the Principle 8 section of The Guide to Data Protection.

Other considerations

Carrying our an assessment of the adequacy of the level of protection for the rights of data subjects is only one method of ensuring a transfer of personal data outside the EEA complies with the Directive.

Guidance on other transfer arrangements is available:

- Using Standard Contractual Terms (Model Contract Clauses)
- Binding Corporate Rules
- International outsourcing arrangements

More Information

This guidance will be reviewed and considered from time to time in line with new decisions of the Information Commissioner, Tribunals and courts.

It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

If you need any more information about this or any other aspect of freedom of information or data protection, please contact us, or visit our website at www.ico.org.uk.