Overseas transfers of personal data
Eighth data protection principle

information commissioner
Barrantagh Fysseree

Advances in technology mean that data is regularly, and frequently, transferred around the world. When such transfers include **personal data**, it is important that the transfer complies with the provisions of the Data Protection Act (DPA) and **all** of the Eight Data Protection Principles.

There are two types of transfer:

1. To a data processor - a third party who processes data on your behalf in accordance with your explicit instructions.

2. To another data controller who determines themselves how that data will be further processed, (but this still cannot be outside the purpose(s) for which it was originally obtained).

In deciding whether to transfer personal data to a **data processor** in a third country, you need to make an informed assessment of the protection that will be afforded in the third country, and also by the data processor, or sub-data processor.

If you are transferring data to another **data controller**, you must also be certain that the personal data will continue to be processed in accordance with the Second Data Protection Principle. It must only be processed for the '*specified and lawful'* purposes for which the data was originally obtained and '*must not be processed in any manner incompatible with that purpose or those purposes.*'

In addition, you must ensure that the processing will be secure and in accordance with the Seventh Principle, which states:

> *'appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to, personal data.'*

This advice note is intended to give guidance on how to make transfers of personal data in compliance with the Eighth Data Protection Principle.

The Eighth Principle states that:

> *'Personal data shall not be transferred to a country or territory outside the Island 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.'*

Making transfers of personal data to third countries

Certain countries or territories ensure an adequate level of protection. These are set out in paragraph 23 of Schedule 1 to the DPA as follows:

1. "a country or territory within the European Economic Area"

   Any country or territory within the European Economic Area (EEA) is conclusively presumed to provide an adequate level of protection. The EEA currently consists of all European Union Member States plus Iceland, Liechtenstein and Norway.

   A current list of EU Member states can be found at http://europa.eu/about-eu/countries/member-countries/index_en.htm

2. "a Community finding has been made in relation to transfers of the kind in question"

   a. The European Commission has made findings recognising that many countries or territories provide an adequate level of protection, including the Isle of Man, Guernsey and Jersey.

      For a current list of "adequate" third countries, please refer to the European Commission website: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

   b. The European Commission has also made findings regarding transfers of personal data relating to US Passenger Names Records (PNR) and for businesses or organisations which are members of the US Department of Commerce' "Safe Harbor" scheme.

      The "Safe Harbor" list can be found on the US Department of Commerce website: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list

If the business or organisation to which personal data is to be transferred is located in any of the countries or a territory mentioned above, or is a recognised type of transfer, then the transfer will comply with the Eighth Data Protection Principle.

How do you ensure an adequate level of protection for transfers to <u>other</u> countries or territories?

You can make a decision as to the adequacy of the third country based on your own assessment of the legal adequacy of the country, and the nature of the personal data you are transferring or exporting and the perceived risk to individuals' personal data, i.e. general adequacy.

To determine what constitutes an adequate level of protection, paragraph 21 of Schedule 1 to the DPA states that the business or organisation should have particular regard to the following:

(a) the nature of the personal data,
(b) the country or territory of origin of the information contained in the data,
(c) the country or territory of final destination of that information,
(d) the purposes for which and period during which the data are intended to be processed,
(e) the law in force in the country or territory in question,
(f) the international obligations of that country or territory,
(g) any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases), and
(h) any security measures taken in respect of the data in that country or territory.

The above means you need to undertake a risk assessment to determine whether, in all the circumstances, the personal data will be adequately protected.

Legal Adequacy

The exporting data controller should consider the following:

- Has the country adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980 or ratified European Convention 108?

- Does it
  - recognise the general rule of law,
  - recognise the ability of parties to bind themselves in a contract,
  - have any legal framework protecting the rights and freedoms of individuals, more specifically relating to the processing of their personal data?

Exporting data controllers are expected to be able to recognise countries where there would be a real danger of prejudice, for example, instability due to war or political reasons, in the third country at the time of transfer. Subsequent, regular checks should continue to be made to ensure that 'adequacy' is maintained. Organisations should also take account of volatility in certain areas of the world and of major world events, reassessing the 'adequacy' as necessary.

General Adequacy Assessment

Using the matrix, consider the following General Adequacy Questions and compare your response with the potential risk you perceive there to be to an individual's personal data.

General Adequacy Matrix

		Level of Potential Risk to an Individual's Personal Data				
		Negligible Risk	Slight Risk	Moderate Risk	Major Risk	Extreme Risk
General Adequacy Question Response	1					
	2					
	3					
	4					
	5					

General Adequacy Questions

- **What is the nature of the personal data that is to be transferred?**
  How sensitive is the personal data on a scale of 1 – 5;
  For example, is it internal telephone extension numbers (1), or health records (5)?

- **What is the purpose of the transfer to the processor in a third country?**
  Is it internal details distributed around a multinational or are these personal details being placed on an Internet site which is accessible by anybody?
  For example, internal = 1 and internet site = 5

- **How long will the personal data involved in the transfer be kept or processed?**
  Will it be used on a single occasion or over a long period of time?
  For example, one occasion = 1, long term, regular use = 5.

- **What technical and security measures does the processor have in place? How do they compare with yours?**
  For example, equivalent to your organisation = 1 and unknown, or poor, level of security = 5

- **Where did the personal data originate?**
  If it was not processed initially by you, where did it come from? Do you know what measures were in place to protect the rights of the data subject at its point of origin?
  *For example, if you are **completely satisfied** that the rights of the individual have been protected = 1, but if you are **completely unaware** what level of protection was afforded= 5*

- **And finally, what is the ultimate destination of the personal data and what protection is afforded there?**
  *For example, you are **completely satisfied** that the rights of the individual will be protected = 1, you are **unsure or are unaware** of what protection is in place = 5*

Can the transfer take place?

If you can satisfy yourself that adequacy can be established either through a Community finding, or by your own adequacy assessment of the risk involved, then the transfer can take place in compliance with the Eighth Data Protection Principle.

If adequacy is not established, or you are in any doubt as to the security provided for the data and for the protection of the rights of the individual, then the exporting controller should examine the use of a contract containing the model clauses as approved either by the European Commission or by the International Chamber of Commerce - http://www.iccwbo.org/ICC_Model_clauses_on_data_transfer/

If you do not use the model clauses, you must record how you ensure compliance with the DPA and be able to justify your actions if they are challenged at a later date.

EC Approved Contract Clauses

The European Commission has approved three sets of standard contractual clauses (known as model clauses) which can be used to provide an adequate level of protection.

These clauses can be found at:
http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm

If you do decide to use the model clauses, **you must use all the clauses** to ensure adequacy.

Binding Corporate Rules

If you are a large multi-national organisation which only transfers personal data within the group, then you may consider using "Binding Corporate Rules". The Information Commissioner cannot approve Binding Corporate Rules as this approval can only be made by an EU Member State data protection authority. For more information, see the UK Information Commissioner's Office guidance at:
http://ico.org.uk/for_organisations/data_protection/overseas/binding_corporate_rules.

The Article 29 Data Protection Working Party has issued a "referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC [Asia-Pacific Economic Cooperation] CBPR [Cross Border Privacy Rules] Accountability Agents" – opinion 02/2014. This document identifies the requirements common or similar to both schemes for approval or certification.

One-off transfers

There will be occasions where the transfer will be subject to derogation, or exemption, from complying with the Eighth Principle; these are set out in Schedule 4 to the DPA.

The derogations are as follows:

- The data subject has already given, and the data controller can provide evidence of, their consent for that transfer.
  Note: Consent may not be appropriate if the transfers are of a long term nature as it can be withdrawn at any time.

- It is **necessary** for the performance of a contract between the data controller and the data subject (e.g. hotel arrangements made by a travel agent for a customer in another country) or the data controller and another third party. In the latter case the data controller must evidence a 'close and substantial connection between the data subject's interests and the purpose of the contract'.

- It is **necessary** 'for reasons of substantial public interest.'

- It is **necessary** in connection with legal proceedings, advice or rights.

- It is in the **vital interest** (matters of life and death) of the data subject, e.g. medical records necessary for the emergency treatment of the data subject.

- If the data forms part of, but not 'the entirety of the data or entire categories of the data contained in', a public register.

These derogations should be construed very narrowly as the provisions reflect the fact that **in these instances only** the transfer must be **necessary** and **justifiable** even though a lower level of, or no, protection will be afforded.