EXTRACT FROM DATA PROTECTION CODE OF PRACTICE

11. INTERNATIONAL TRANSFERS OF PERSONAL DATA

Under the DPA 1998, there are different legal requirements for contracts depending on which country the data will be held in. The most important distinctions are whether information will be held:

- within the EEA
- by a country on the European Commission's approved list; or
- in another non-EEA country.

11.1 Transfers of Personal Data to European Economic Area (EEA) Countries

The countries which constitute the EEA are the 28 members of the European Union, together with Lichtenstein, Norway and Iceland. The full list is available at: http://europa.eu/abc/european_countries/index_en.htm

These countries are considered to ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. This means that transfers of personal data between those countries are automatically permitted.

However it is unwise to assume that transfers of personal data to, or from, other EEA States will always be straightforward. Prior to beginning any personal data transfers to EEA States, University staff should:

- Evaluate the relevant national legal and administrative compliance criteria for personal data transfers in all countries involved
- Liaise with appropriate officers in institutions/organisations to, or from, whom data is to be transferred, to allocate responsibility for ensuring that appropriate legal and administrative formalities have been satisfied
- Document both the legal and administrative requirements, and the agreed responsibilities of the respective parties, ideally in a contractual document, with appropriate warranties and indemnities in case of breach

Template clauses to incorporate into an existing agreement and a separate standalone template agreement are available from Governance Services.

11.2 EU Commission Approved List

11.2.1 Some countries outside the EEA have been officially deemed by the EU Commission to have an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The EU Commission publishes a full list of approved countries, which includes Argentina, Canada, Switzerland, Guernsey and the Isle of Man.

11.2.2 There is a partial finding of adequacy for the United States with regard to those organisations who have volunteered to be subject to the EU-US Privacy Shield scheme.

11.2.3 Where the country has been formally assessed as providing adequate protections, the transfer is to be treated as a data transfer to an EEA country and the template clauses and agreements referred to in 11.1 above are to be used.

11.3 Transfers of Personal Data to Non-EEA Countries

The DPA 1998 contains specific provisions with regard to the transfer of personal data to countries outside the EEA. The eighth data protection principle states "'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." This is qualified by a number of conditions e.g. personal data may be transferred to a country without an adequate level of protection where the data subject has given consent to the transfer.

11.3.1 University staff should ensure that there are clear and documented procedures and administrative responsibilities for the transfer of personal data to non-EEA countries. University staff should consult this checklist when considering if a transfer of personal data is proposed.

11.4 Exceptions to Prohibition on Data Transfer

The DPA 1998 provides a number of exceptions to the prohibition on the transfer of the personal data in question, details of which are given with the checklist above.

11.4.1 Use of exceptions

Any use of these exceptions must be fully documented in order to justify the basis for any transfer made to a third country, in case of a challenge made by either the ICO or in the courts.

11.5 Consent

The potential benefits of obtaining specific and informed consent of data subjects before the transfer of data to a non-EEA country are:

- The data subject can be made aware of the risks that the University may have assessed as being involved in the transfer; and
- The data subject is able to give their clear and unambiguous consent to the transfer

Examples would include the transfer of staff personal data to a non-EEA country to be used in the management of a distance learning course and where a data subject requests a reference be written and sent to a non-EEA country. In the latter case the request itself will indicate consent to the personal data transfer.

Staff involved in any transfers where consent is relied upon as the justification for the data transfer must ensure that they:

- document that the data subject was informed as required
- obtain consent in writing, unless there are suitable technological means to ensure that authenticated consent can be collected on-line
- retain evidence of both the above

11.6 Method of Transferring Personal Data

Where it has been established that personal data may be transferred, this should be done in accordance with section 7.5 of this Code of Practice; electronic transfers of personal data must be encrypted. IT Services provide guidance on both Data Encryption and on Email Encryption.

11.7 Third Party Requests

University staff must ensure that personal data is not disclosed without the specific and informed consent of the data subjects concerned when requested by:

- non-EEA governments, agencies, and organisations for the purposes of assessing the names, numbers and whereabouts of foreign nationals studying overseas where there is no sponsorship arrangement or other agreement between the data subject and a third party
- non-EEA governments for the purposes of determining liability to attend National Service

11.8 Data Controller Assessment of Adequacy for Non-EEA Transfer

Where none of the above options apply for a transfer outwith the EEA, the University may determine that the transfer it wishes to make will provide adequate safeguards. However this must be discussed at the outset with Governance Services who will seek any necessary legal advice and ensure that the relevant area conducts a risk assessment.

11.9 Further Information on International Transfers

The UK Information Commissioner has provided the following guidance:

- **Can I Send Personal Data Overseas?**
  https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/