Guidance on Transferring Personal Data outside the European Economic Area

1. Introduction

Data protection legislation prohibits the transfer of personal data to countries outside the European Economic Area (**EEA**) unless:

- The country in question has been deemed by the European Commission to provide an adequate level of protection for personal data; or

- One of the mechanisms set out in the legislation has been put in place applies, e.g. where one of the 'appropriate safeguards' listed in data protection legislation has been put in place or a specific exception applies (see below for further detail on this point).

These restrictions are in place because countries outside the EEA are deemed not to provide an adequate level of protection for personal data.

This note explains the restrictions applicable to transfers outside the EEA and the steps that UCL staff must take in order to ensure that any transfers comply with data protection law. It is designed to be read in conjunction with the other data protection guidance available on our website here.

This document was last updated on 2 November 2018. It may be updated further as relevant guidance on the issues raised is published by the UK Information Commissioner's Office (**ICO**).

2. Scope

Personal data

This guidance applies only where UCL is transferring personal data (i.e. information that relates to an identified or identifiable individual) to a country outside the EEA.

The restrictions do not apply to fully anonymised data, which cannot be used to identify individuals even when combined with other information which is available to the recipient of the data.

The EEA

As of October 2018, the following countries are within the EEA: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK (see here for further information).

3. Steps to take before making a transfer outside the EEA

You should consider the following steps before making the transfer:

Step 1 – Are the data personal data?

Determine whether you are processing personal data. Here is the definition:

> *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*

Step 2 - Necessity test

Is the processing of personal data is 'necessary' for achieving the objective. 'Necessary' in this context means that the processing should be a targeted and proportionate way of achieving your objective. It may be that there is another way of achieving the objective. If there is no other way, then clearly the processing is necessary. If there is another way but it would require disproportionate effort, then you may determine that the processing is still necessary.

Ask yourself is it necessary to transfer the personal data outside the EEA, or could you achieve your objectives without doing so? For example you may be able to meet your objectives by transferring anonymised data only or you may not need to transfer any data at all.

Step 3 – Transit or transfer?

Are you transferring the data to a country outside the EEA or will it be just in transit through a non-EU country? If data is only in transit through a non-EEA country (and is not accessible), this will not constitute a transfer outside the EEA.

Step 4 – Data protection principles

Having determined that you are transferring personal data, have you complied with all of the other data protection principles? If you transfer personal data outside the EEA, you are required to comply with all relevant data protection requirements and all applicable UCL policies and procedures, not just those relating transfers outside the EEA.

Step 5 – Consider whether you need a data privacy impact assessment (DPIA)

Follow this guidance.

Step 6 - Compliance with data protection legislation (adequacy decision)

Under current data protection law, transfers outside the EEA may only be made in specific circumstances. The circumstances most likely to be of relevance where UCL transfers data outside the EEA are set out below.

You should work through the following scenarios in order, considering whether that basis for the transfer will apply before moving onto the next scenario.

i. Has the European Commission made an adequacy decision in respect of the relevant country or territory?

The first thing that you should check before making the transfer is whether an 'adequacy decision' is in place in respect of the relevant country or territory.

If an adequacy decision has been made in respect of the country to which you are transferring personal data, then you will not need to take any further steps in order to make the transfer (although you must continue to comply with all relevant provisions of the data protection legislation and all applicable UCL policies and procedures).

A full adequacy decision has been made in respect of the following countries and territories:

- Andorra;
- Argentina;
- Guernsey;
- Isle of Man;
- Israel;
- Jersey;
- New Zealand;
- Switzerland; and
- Uruguay.

The adequacy decision therefore applies where personal data is transferred to any type of organisation within these countries/territories.

The Commission has made partial findings of adequacy about Canada and the USA:

- **Canada:** the adequacy finding for Canada only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (**PIPEDA**). Not all data is subject to PIPEDA. If you require assistance in determining whether PIPEDA is applicable, please contact the UCL Data Protection team using the contact details set out below.

- **USA:** The adequacy finding for the USA only relates to organisations which are certified members of the EU-US Privacy Shield framework. If you want to transfer personal data to a US organisation under the Privacy Shield, you will need to:

    - Check the Privacy Shield list to see whether the organisation has a current certification; and

    - Make sure the certification covers the type of data you want to transfer.

Step 7 - compliance with data protection legislation (no adequacy decision)

If no adequacy decision has been made, ie the country you want to transfer personal data to is not in the list in step 5 above, you will need to consider whether:

- One of the 'appropriate safeguards' set out in data protection legislation applies (see section (a) below; or

- If not, whether a specific exception set out in data protection legislation applies (see section (b) below).

a) Appropriate safeguards: standard contractual clauses

What are the standard contractual clauses?

Several 'appropriate safeguards' are listed in the General Data Protection Regulation (**GDPR**). The one that is most relevant to transfers carried out by UCL is the 'standard contractual clauses', also known as 'model clauses' which have been approved by the European Commission.

UCL (as a 'data exporter') and the recipient of the personal data (as a 'data importer') will need to sign a standard form agreement before any transfer of personal data outside the EEA occurs.

There are different sets of standard contractual clauses depending on whether there is 'controller to controller' transfer or 'controller to processor' transfer. The correct set must be used.

- For controller to controller transfers, please use **these** standard contractual clauses.

- For controller to processor transfers, please use **these** standard contractual clauses.

Can I make amendments to the standard contractual clauses?

You must not make amendments to the wording of the standard contractual clauses (although additional commercial clauses may be added, such as optional indemnity wording). Details of the processing activities will also need to be included, as specified in the relevant set of standard contractual clauses. Please contact the data protection team for further guidance on completing the standard contractual clauses.

Can the standard contractual clauses be used if UCL's processor based in the EEA wishes to transfer personal data to a sub-processor outside the EEA?

You should first check whether that sub-processor is located in a country or territory in respect of which an adequacy decision has been made. If not, standard contractual clauses should be used. However, there are currently no standard contractual clauses designed for use between a processor and a sub-processor. This means that where UCL transfers personal data to a processor within the EEA who will then transfer personal data to a sub-processor outside the EEA, the standard contractual clauses should be put in place between UCL and the sub-processor. Please contact the data protection team for further guidance on this issue.

b) Exceptions

Data protection law sets out certain exceptional circumstances in which a transfer may take place, even where no adequacy applies and no appropriate safeguards can be put in place. Below is a brief summary of three exceptions:

- **Consent:** a transfer may be made where the individual has given their explicit, fully informed consent to a specific transfer;

- **Contract:** transfers may be made where necessary for the performance of a contract: (a) between the individual and UCL or for pre-contractual steps taken at the individual's request; or (b) made in the interests of the individual between UCL and a third party; and

- **Legal claims:** a transfer is allowed where it is necessary for the establishment, exercise or defence of legal claims.

However, the 'consent' and 'contract' grounds may not be relied upon by public authorities (including universities) in the exercise of their public powers. This means that it is very unlikely that UCL will be able to rely on these exceptions in most circumstances. Please contact the data protection team for further advice if you are considering relying on an exception.

4. Further guidance

If you require any further information on the issues raised in this document, please contact the data protection team at data-protection@ucl.ac.uk.