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 and 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 (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

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

- 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).

urpa

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