

International transfers

Guidance regarding transferring personal data from the University to a country outside the UK.

Audience

This guidance is intended for the Data Protection Champions and University staff who send personal data from within the University to an institution, a person or an organisation outwith the UK.

Introduction

The UK General Data Protection Regulation (UK GDPR) sets out that personal data may only be transferred outside of the UK when certain safeguards are in place. These safeguards are divided into two categories: 'regular' safeguards available to all data controllers and the so-called derogations, the exceptions that are only available to public authorities if the transfer falls outside their public tasks. Therefore, activities which the University has no delegated powers to undertake can continue to make use of these derogations to simplify overseas data transfers. However, teaching and research are public tasks, which the University has delegated authority to undertake.

Please note that transfer of personal data into the UK is unproblematic, as Data Protection Laws will apply as though the data were generated inside the UK.

Please note that accessing University systems by a University staff member from abroad does **not** constitute international data transfer.

Context

Under the UK GDPR and DPA 2018, these safeguards are not required where the European Commission ("the EC") has decided that a country, territory or a sector(s) within a country has an adequate level of protection ("an adequacy decision") over personal data. Where an adequacy decision is available, transfers of personal data can take place as if the recipient were located within the EEA ("the EEA"), i.e. no further actions are required other than general compliance with the legislation. The UK will recognise and adopt these adequacy decisions; in addition, the UK will recognise all EEA countries as adequate.

To date, the EC has recognised Andorra, Argentina, Canada (only commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and Japan as providing adequate protection.

Many of the University's overseas partnerships allow for the free transfer of personal data, as these involve institutions/bodies within the EEA. However, the University also shares personal data with institutions in countries with no EC adequacy decisions in place.

Please note that the EU has recognised the UK as adequate post Brexit.

Several scenarios involve the transfer of personal data outwith the EEA and the adequate countries:

- Regular student exchange
- Teaching and/or activities delivered by an institution overseas
- International research collaborations
- International conferences and events
- Work placements
- External examiners
- Student or staff references

- Providing membership data to professional organisations or similar organisations
- Overseas development and alumni work
- Providing data to an embassy for a very important person (VIP) visit

The legislation lists 8 safeguards, at least one of which must be put in place to allow for the lawful transfer of personal data to non-adequate countries.

Adequate safeguards may be provided for by:

1. a legally binding agreement between public authorities or bodies;
2. binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
3. standard contractual clauses adopted by the EC;
4. standard contractual clauses adopted by the Information Commissioner's Office (ICO);
5. compliance with an approved code of conduct approved by the ICO;
6. certification under an approved certification mechanism as provided for in the GDPR;
7. contractual clauses agreed authorised by the ICO;
8. provisions inserted into administrative arrangements between public authorities or bodies authorised by the ICO.

Note: The decision by the European Court of Justice from July 2020 invalidated the Privacy Shield for data transfer to the US and added requirements for use of the standard contractual to be inserted into contracts. A risk assessment must now be completed and approved by the Head of College respectively Director of Support Area or their representatives whenever these clauses are to be used. The risk assessment needs to consider whether it is likely that the data will be accessed by, for example government agencies in the recipient country such as under the Patriot Act in the US. This risk assessment is contained in one of the questions in the DPIA. The DPO will approve the DPIA and then send it on to the Head of College respective Director of Support Area for approval of that question.

Besides the 8 safeguards, there are 7 derogations, which are alternatives to the application of a safeguard. It is important to note that the derogations are exceptions and must be used accordingly, only where necessary for exceptional situations and not for regular data transfer. Where available, a derogation can only be relied upon when there is no adequacy decision and application of a safeguard is not possible, or desirable, e.g. establishing a contract between the University and another party for a one-time transfer would not be an efficient use of resource; with no guarantee that the partner would accept the terms a proposed agreement.

The derogations are:

1. the individual's informed written consent;
2. necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
3. necessary for the performance of a contract made in the interests of the individual between the controller and another person;
4. necessary for important reasons of public interest;
5. necessary for the establishment, exercise or defence of legal claims;
6. necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
7. made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

Note that the first three derogations, explicit consent and the two contractual derogations, only apply to the University's so-called private tasks, i.e. any task outwith teaching and research.

Safeguards for international transfer – individual situations**Regular student exchange (incoming and outward bound students):**

If the other university is a public body: a legally binding agreement between public authorities

If the other university is private: necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request.

Teaching and/or activities delivered by an institution overseas:

Teaching and/or research activities delivered by an institution overseas that rely on a personal data transfer from the University of Edinburgh fall outwith the scope of our GDPR compliance, as the University of Edinburgh will not be undertaking any activities under its own powers – it will be the other institution that is doing so.

International research collaborations:

If the other university is a public body: a legally binding agreement between public authorities.

If the other university is private: standard contractual clauses.

International conferences and events:

Informed written consent.

Work placements:

Necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request.

External examiners:

Necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request.

Student or staff references:

Necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request.

Providing membership data to professional organisations:

Informed written consent.

Overseas development and alumni work:

Informed written consent.

Providing data to an embassy for a VIP visit:

Necessary for important reasons of public interest.

Guidance:

For advice on contracts and legally binding agreements, please consult Legal Services at legalservices@ed.ac.uk

Further guidance on consent is available on our website:

[Guidance on consent](#)

The Information Commissioner's Office also provides guidance on international transfers.

[Information Commissioner's Office guidance on safeguards and derogations](#)

About this guidance

Version control	Author/editor	Date	Edits made
1	Data Protection Officer	3 December 2018	Wrote guidance

Version control	Author/editor	Date	Edits made
2	Deputy Information Compliance Manager	6 December 2018	Formatted for web and accessibility
3	Data Protection Officer	24 August 2010	Added guidance on international transfer to USA.

If you require the guidance in an alternative format, please contact the Data Protection Officer: DPO@ed.ac.uk or 0131 651 4114.