EDINBURGH NAPIER UNIVERSITY

GUIDANCE ON THE CONTRACTUAL REQUIREMENTS FOR TRANSFERRING PERSONAL DATA TO EXTERNAL ORGANISATIONS

What is the purpose of this guidance?

This guidance provides general advice on the issues you need to consider when setting up or managing contracts where you intend to transfer personal information from the University to another organisation. This is to ensure that you do so in a way that complies with current Data Protection legislation: the EU General Data Protection Regulation (GDPR)(Regulation (EU) 2016/679) and UK Data Protection Act 2018 (DPA 18) (hereafter referred to collectively as Data Protection legislation).

It is part of a set of guidance that you can use to ensure compliance with Data Protection legislation. The complete guidance consists of this page, an explanation about the European Economic Area (EEA), information about what exemptions may apply to allow you to transfer data outside the EEA and finally advice on each of the four possible scenarios for transferring data and the model contract clauses to use in those cases.

For whom is this guidance intended?

This guidance is intended for all University staff responsible for managing or establishing relationships with external organisations, where the relationship involves either passing information about living, identifiable individuals to that organisation, or giving the organisation access to such information held by the University.

Why does Data Protection legislation affect my arrangements for passing information to other organisations?

Data Protection legislation is concerned with personal data. As the precise definition of personal data is complex it is best to assume that all information about a living, identifiable individual is personal data. (See also the section below on “What is personal data?”) The legislation gives individuals rights regarding the personal data the University holds about them and imposes responsibilities on the University regarding its use of that data. These responsibilities are contained in the data protection principles.

Any transfer of personal data from the University to another organisation must comply with these principles and a contract is the best way to ensure that they do.

What steps should I take when setting up a relationship with an outside organisation that will involve the transfer of information about living, identifiable individuals?

You should do the following:

a. Decide whether or not the transfer involves personal data.
b. If it does, decide whether the other organisation is a data controller or a data processor.
c. Establish in which countries the other organisation will hold any information the University gives to it. You will need different arrangements for different countries.
d. Use this guidance and the information you have gathered to decide which of the contractual clauses you need to use.

What is personal data?

The definition of personal data, and the extent to which the data protection principles apply to it, is very technical. When setting up a relationship with an outside organisation that involves the transfer of information about living, identifiable individuals, you should look first at the definition of personal data in s. 2.2 of the Data Protection Act Code of Practice:

If necessary you should then check the UK Information Commissioner's guidance on this.

What is a data controller?

A data controller is an organisation that has full authority to decide how and why personal data is to be "processed" (this includes using, storing and deleting the data). When the University decides that it wishes to pass the personal data it holds to another organisation, the University is acting as a data controller as the University has the authority to take this decision.

Further information on the definition of a data controller is available in s. 2.5 of the Data Protection Act Code of Practice

Whether or not the receiving organisation is also a data controller will depend on whether or not that organisation will have the authority to decide how and why the data will be stored, used and deleted. If the receiving organisation has considerable discretion in this area, it is probably a data controller.

For example, information such as the destinations of leavers which is passed by the University to HESA for analysis is done so as a data controller to data controller transfer. This is because HESA is a separate organisation and will be using the data for their own purposes, purposes that the University will not be involved in or have control over.

What is a data processor?

A data processor is an organisation that "processes" personal data on behalf of another organisation. Processing includes collecting, reading, amending, storing and deleting.

Further information on the definition of a data processor is available in s. 2.6 of the Data Protection Act Code of Practice

If the University passes personal data to an organisation but retains the right to specify what should be done with that data, then the receiving organisation is a data processor. The University is legally responsible for any breaches of Data Protection legislation committed by any data processor acting on its behalf and can be sued if a data subject suffers damage as a result of any breach.

For example, if information held in University databases is passed to an external company for scanning and digitising purposes the company contracted to carry this out will be a data processor as the University will retain control over the data and the purposes for which it is processed. It is essential therefore that the relevant agreement contains all the necessary safeguards and the University has a duty to monitor the agreement, which may include a site visit where appropriate.

What is data processing?

The UK Information Commissioner (UK ICO) has advised that any action taken with regard to personal data will amount to processing of that data. A more detailed definition is given in s. 2.7 of the Data Protection Act Code of Practice

What measures do I need to take to ensure data protection compliance?

There are four different scenarios that might arise. This guidance will help you to choose which set of clauses are most appropriate for your circumstances when you propose to transfer data from the University to:

1. A data processor in the UK, EEA or on the approved list
2. A data processor outside the EEA and not on the approved list
3. A data controller in the UK, EEA or on the approved list
4. A data controller outside the EEA and not on the approved list

If possible, avoid establishing a relationship where the University is the data controller and the other organisation is the data processor. If you cannot do this, you must build safeguards into the contract to limit the University's exposure to risk.

Why does it matter where the other organisation will hold the information?

Under Data Protection legislation there are different legal requirements for contracts depending on which country the data will be held in. The most important distinction is whether information will be held within the European Economic Area (EEA), by a country on the European Commission's approved list or in another country.

Article 46 of the GDPR states a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Which countries are in the EEA and on the approved list?

Countries in the EEA

Countries on the European Commission's approved list

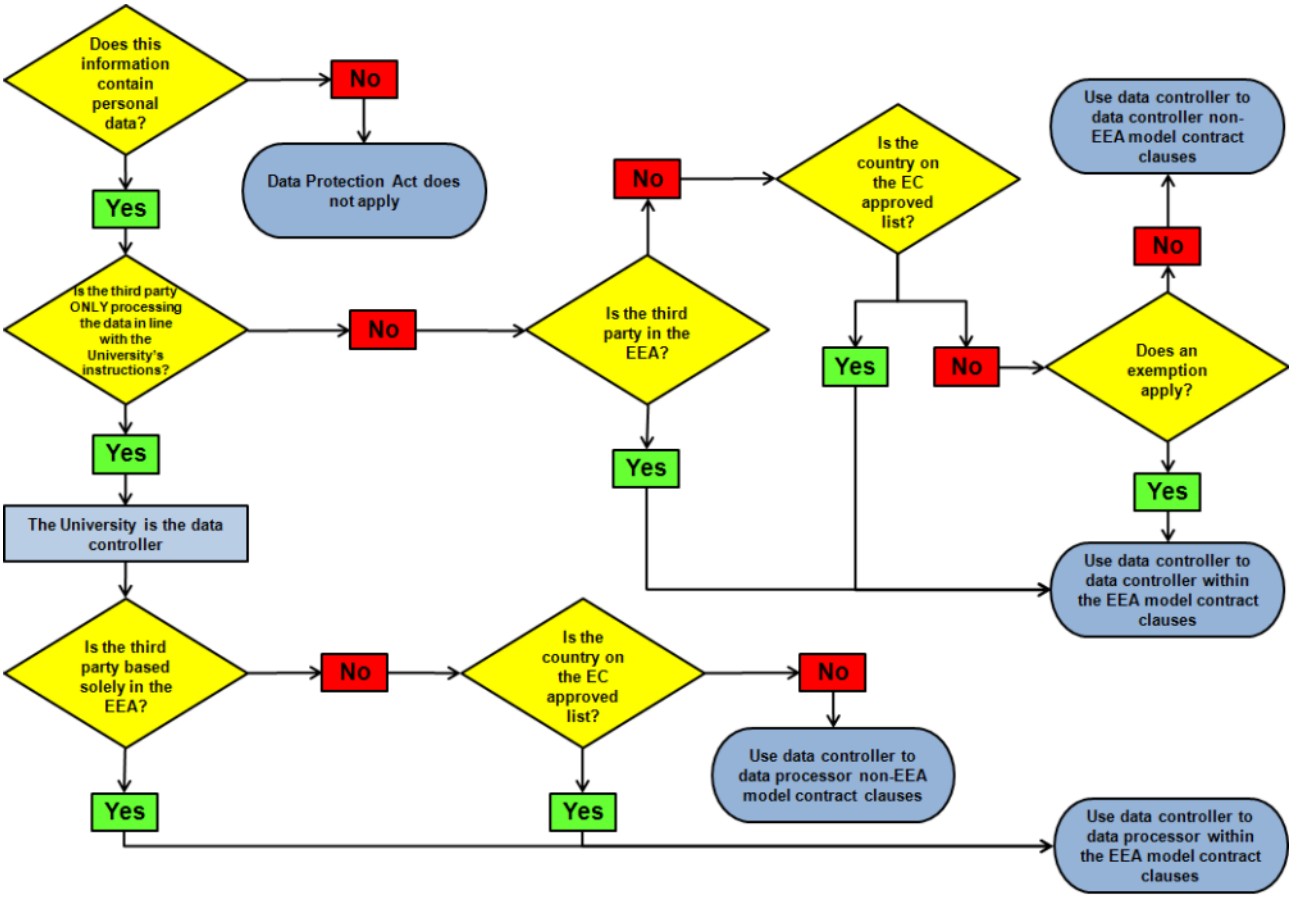
The UK ICO also publishes guidance on assessing a country's adequacy for International Transfers.

When do exemptions to the prohibition on transfers of personal data outside the EEA apply?

Exemptions to the prohibition on transfer outside the EEA will mostly likely occur when information is transferred to another data controller. Further information about these is contained in this checklist.

What clauses should I use?

The following flowchart will help you to decide this:



There is a larger format PDF version of this flowchart. The Governance Officer (Data Protection & Legal) can advise further and provide template clauses.

Edinburgh Napier University gratefully acknowledges the University of Edinburgh's permission to use and adapt their published materials in the preparation of this guidance.

Governance Services
Updated September 2018