Overseas Transfers & Hosting

Title	Overseas Transfers & Hosting
Status	Approved
Version	V1.0
Date Approved	21st May 2020
Review Date	21st May 2021

Contents

1. Introduction

When a Data Controller uses personal data, either itself or via a Data Processor, to deliver services which require handling personal data, the law makes clear that the Data Controller is still legally responsible for that data and that the Data Processor can only act on the Data Controller's instructions under a 'written contract'

It is important that if transfers of personal data are made to overseas countries, or you procure the services of a suppliers whose datacentres and/or support services are located in an overseas country, that you comply with your legal obligation to ensure appropriate safeguards are in place to protect personal data. Data subjects must be assured that the same level of protection and the same rights will apply to the processing of their personal data overseas as it would if the data were processed in the UK.

The principle that the law introduces is this:

- If the Controller fails to have appropriate safeguards in place it is unlawful processing and therefore a personal data breach.
- Overseas transfers/hosting must be explained in your privacy notices and documented in your Records of Processing Activity and Data Protection Impact Assessments.
- Regulatory action (including monetary penalties) is taken against Controllers and also, where there is failure to follow instruction from Controllers, against Processors.

2. Quick Reference Guide

- All data transferred, stored or processed outside the UK must be identified and documented in your Records of Processing Activities (RoPA)
- *Until 31st December 2020 transfers to EU countries do not required additional safeguards. Only personal data coming into the UK from EU countries will be affected during this period.*
- Where the transfer relates to student information, ensure you have consent from the Parent/Carer and where the child is twelve years of age or older, the child themselves. When gaining consent you must explain any risks to the personal data associated with the transfer to enable their consent to be informed
- Always record the informed consent and your rationale/justification for sending the personal data overseas
- When transfers relate to service provision e.g. Cloud services or systems, always ensure that you have a written contract with the supplier, or other agreement which is legally binding

- Where personal data will be transferred, received or stored in overseas countries ensure that, where the transfer is subject to a contractual arrangement, your contract includes the ICO approved Standard Contract Clauses
- Completing a Data Protection Impact Assessment will guide you to consider what assurances you need from any overseas supplier you wish to enter into a contract or agreement with
- Ensure you have documented which safeguards you will be relying on to support overseas transfers in your Privacy Notices and Records of Processing Activity.

3. Policy References

3.1. This procedure is a requirement of the following policies:

- Data Protection Policy

4. Procedures

4.1. Appropriate Safeguards

4.1.1. The first step is to establish a list of all the overseas organisations (and potentially some individuals) who you give (or allow them to access on your behalf) the personal data for which you are Data Controller. Once these data flows are identified you can assess which of the safeguards permitted by law apply for each flow.

4.1.2. The list of safeguards includes:

a) An Adequacy Decision
b) ICO Approved Standard Contract Clauses
c) Exceptions to the Safeguards for Overseas Transfers

Adequacy Decisions

An adequacy decision is where an authorising body (in this case the ICO) accept an overseas countries evidence that they have in place the right laws to ensure that personal data processed in their country is subject to a sufficiently high level of protection, and that data subjects have the same rights as those in the UK. The ICO publish a list of countries with an adequacy decision, these currently include:

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

There are partial findings of adequacy about Japan, Canada and the USA.

- The adequacy finding for Japan only covers private sector organisations.
- 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.
- The adequacy finding for the USA is only for personal data transfers covered by the EU-US Privacy Shield framework.

The Privacy Shield places requirements on US companies certified by the scheme to protect personal data and provides for redress mechanisms for individuals. US Government departments such as the Department of Commerce oversee certification under the scheme.

If you want to transfer or store personal data to a US organisation under the Privacy Shield, you need to:

- check on 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.
- *After 31st December 2020 the US organisation will have to have updated their public commitment to expressly state that it applies to transfers from the UK.*

You can view an up to date list of the countries which have an adequacy finding on the ICO website. You should check back regularly for any changes.

ICO Approved Standard Contract Clauses

The ICO standard contract clauses are available at Annex A. These clauses cannot be altered and must be used in full. Both parties must retain a copy of these clauses. The clauses can be added into an existing contract or included in a new contract.

Exceptions from the Safeguard requirements for Overseas Transfers

Where none of the above safeguards apply to the overseas transfer you should consider whether an exception from the need for these safeguards is applicable. Those exceptions are:

a) Explicit Consent

As a valid consent must be both specific and informed, you must provide the individual with precise details about the restricted transfer. You cannot obtain a valid consent for restricted transfers in general.

You should tell the individual:

- the identity of the receiver, or the categories of receiver;
- the country or countries to which the data is to be transferred;
- why you need to make a restricted transfer;
- the type of data;
- the individual's right to withdraw consent; and
- the possible risks involved in making a transfer to a country which does not provide adequate protection for personal data and without any other appropriate safeguards in place. For example, you might explain that there will be no local supervisory authority, and no (or only limited) individual data protection or privacy rights.

b) It is necessary to perform a contract

This exception explicitly states that it can only be used for **occasional** restricted transfers. This means that the restricted transfer may happen more than once but not regularly. If you are regularly making restricted transfers, you should be putting in place an appropriate safeguard.

The transfer must also be **necessary**, which means that you cannot perform the core purpose of the contract or the core purpose of the steps needed to enter into the contract, without making the restricted transfer. It does not cover a transfer for you to use a cloud-based IT system.

c) It is necessary to make or defend a legal claim

This exception explicitly states that you can only use it for **occasional** transfers. This means that the transfer may happen more than once but not regularly. If you are regularly transferring personal data, you should put in place an appropriate safeguard.

The transfer must be necessary, so there must be a close connection between the need for the transfer and the relevant legal claim.

The claim must have a basis in law, and a formal legally defined process, but it is not just judicial or administrative procedures.

d) A one-off transfer which is in your compelling legitimate interests

If you cannot rely on any of the other exceptions, there is one final exception to consider. This exception should not be relied on lightly and never routinely as it is only for truly exceptional circumstances.

For this exception to apply to your restricted transfer:

- there must be no adequacy decision which applies.

- you are unable to use any of the other appropriate safeguards. You must give serious consideration to this, even if it would involve significant investment from you.
- none of the other exceptions apply. Again, you must give serious consideration to the other exceptions. It may be that you can obtain explicit consent with some effort or investment.
- your transfer must not be repetitive – that is it may happen more than once but not regularly.
- the personal data must only relate to a limited number of individuals. There is no absolute threshold for this. The number of individuals involved should be part of the balancing exercise you must undertake in para (g) below.
- The transfer must be necessary for your compelling legitimate interests. Please see the section of the guide on legitimate interests as a lawful basis for processing, but bearing mind that this exception requires a higher standard, as it must be a compelling legitimate interest. An example is a transfer of personal data to protect a company's IT systems from serious immediate harm.
- On balance, your compelling legitimate interests outweigh the rights and freedoms of the individuals.
- You have made a full assessment of the circumstances surrounding the transfer and provided suitable safeguards to protect the personal data. Suitable safeguards might be strict confidentiality agreements, a requirement for data to be deleted soon after transfer, technical controls to prevent the use of the data for other purposes or sending pseudonymised or encrypted data. This must be recorded in full in your documentation of your processing activities.
- You have informed the ICO of the transfer. We will ask to see full details of all the steps you have taken as set out above.
- You have informed the individual of the transfer and explained your compelling legitimate interest to them.

5. Record keeping

It is vital in order to meet the Accountability Principle that all overseas transfers are fully documented. Such transfers must be referenced in:

- Your Privacy Notices
- Your Records of Processing Activity
- Your Risk Register
- Your Processor Evidence Files

5.1. Privacy Notices

Where you will be transferring personal data outside the UK, the law requires you to tell people this, and explain what safeguards are in place to secure the data. At the point of collection, or as soon as you receive the personal data you must make the data subjects aware of their rights and how their data will be processed; including any overseas transfers. Privacy notices are commonly held on an organisation's website, and data collection forms provide signposting to them. Ensure each relevant notice is updated to reflect any overseas transfers explaining:

- Which processing is affected
- Who any data processors are
- Which country the data will be processed in
- What safeguards are in place to protect the data

Your general privacy notice must make clear how individuals can exercise their rights and how to make complaints.

5.2. Records of Processing Activity

To comply with data protection law you must maintain records of processing activity. An element of this is the mapping of your data flows. Where data is transferred or received from overseas you must state which countries are involved. Please ensure you complete **column BF of your RoPA** with the type of safeguard you will be using for each overseas flow.

5.3. Risk Register

Typically, the high-risk processing will involve processing of personal data that meets the requirement to undertake a Data Protection Impact Assessment (DPIA) (Document G4). Previously known as a Privacy Impact Assessment and recommended as good practice by the Regulator (the Information Commissioner Office (ICO)), GDPR now requires these to be undertaken by law if your proposed processing poses "a high risk to the rights and freedoms of" data subjects (Article 35).

The term "high risk" is not well defined in the law, but as a rule of thumb, wherever your proposed processing involves Special Category (sensitive personal) data, or there are other risks, e.g. overseas transfers, then undertaking the DPIA process is advised. The process is a risk assessment, prompting you to consider how your new service or system is going to remain compliant with the law. It will capture the details of the safeguards you will apply to overseas transfers. Use document G5 to guide you through the risk assessment.

It is advisable to engage with your Data Protection Officer (DPO) as early as possible in this process as the law requires the School to seek the DPO's advice.

There should be evidence of the DPO's involvement, e.g. an approval 'sign-off' in order to satisfy the legal requirement.

5.4. Processor Evidence Files

Where your suppliers provide services, e.g. hosted solutions, overseas you must ensure that there is a formal contract. Where the recipient/sender country does not have an adequacy decision you will also need to consider using the ICO Standard Contract Clauses. You should keep all documentation for all Processors in an Evidence File (or collection of files) for ease of review.

6. Advice and Support

If you have any issues over the clarity of these procedures, how they should be applied in practice, require advice about exemptions from the requirements or have any suggestions for amendments, please contact the school office.

7. Breach Statement

A breach of this procedure is a breach of Information Policy. Breaches will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Annex A:

ICO-SCCs