Information Governance Framework for International Data Transfers

Introduction

This Information Governance Framework for International Data Transfers (the Framework) is designed to guide staff through the Data Protection and other Information Governance factors to consider at the outset/proposal stage when considering a project; contract or initiative involving the processing of personal data outside of the UK. It ensures that the complex legal requirements are followed; adequate controls are in place from the very start of the work and gives enough time for the required documentation to be put in place.

This Framework must be completed prior to the international transfer of personal data and agreed with the Information Governance team (dpa@abdn.ac.uk), unless advice has been provided by the Data Protection Officer to the contrary.

In the absence of an adequacy decision (explained further below), the University may transfer personal data to a third country or an international organisation only if an appropriate safeguard is in place AND on condition that enforceable data subject rights and effective legal remedies for data subjects are available. There are a number of 'appropriate safeguards', listed in Article 46 of the UK GDPR, which can be used in this context:

- A legally binding and enforceable instrument between public authorities or bodies (approved by the Information Commissioner's Office);
- Binding corporate rules;
- An approved code of conduct or certification mechanism;
- An International Data Transfer Agreement (IDTA).

In the majority of cases, the University will seek to rely on the IDTAs, formerly known as Standard Contractual Clauses (SCCs). These are the UK equivalent of EU SCCs, which came into force on 21 March 2022, and can comprise a stand alone IDTA or an addendum IDTA to existing SCCs.

In order to rely on an appropriate safeguard including the IDTA, it is a legal requirement that, in addition to the IDTAs being drafted and signed, a document known as a Transfer Risk Assessment (TRA) must be carried out. The TRA applies to routine data transfers out of the UK and the transfer may only proceed where either the transfer causes no risk or a low risk of harm to data subjects, taking into account any appropriate steps and protections put in place via the TRA to reduce the risk to low.

More complex arrangements may require a Data Protection Impact Assessment alongside the TRA. This Framework, including Checklist, is designed to ensure that the correct processes are in place prior to the transfer.

Contents of Framework

This Framework comprises the following:

- Checklist for completion by School/Directorate lead;
- Annex 1 – Guidance for completion of the Checklist;
- Annex 2 - Transfer Risk Assessment (to be completed by the Information Governance Team only with assistance and sign off from the School/Directorate lead);

- Annex 3 – Other Information Governance Requirements.

YOU ARE ONLY REQUIRED TO COMPLETE PAGES 3 & 4 OF THE CHECKLIST TO THE EXTENT POSSIBLE

Scope

This Framework covers the sharing of personal data outside the UK in any scenario, but will include: exchange programme or joint initiative; via participation in an international research programme; where a supplier intends to host University personal data outside the UK. It supplements the University's Data Protection policy and the Data Protection guidance pages available on Staff Net.

If you have any queries regarding the scope and application of this Framework to your own project or for assistance with data protection requirements for a specific international project, please contact the Information Governance team at **dpa@abdn.ac.uk**

Escalation of Risk

This Framework is designed to assess and document the lawful process for the international data transfer and ensure that steps are taken to reduce any risks to individuals (data subjects) to minimal. In the event that the Framework indicates at any stage that a less than minimal risk to data subjects exists which cannot be mitigated or a provision cannot be found which permits the restricted transfer to take place in accordance with the Data Protection Legislation but that the Project Sponsor or Information Asset Owner nonetheless wishes the transfer to take place, the following will be adhered to:

- The Data Protection Officer shall report the matter to the next available meeting of the Information Governance Committee or International Partnership Committee;
- Following the outcome of that meeting, the Data Protection Officer shall update the relevant Project Sponsor or Information Asset Owner;
- In the event that an urgent response is required prior to the next Committee meeting, the matter shall be escalated to the Information Governance Committee either via email circulation or a single item virtual meeting;
- Relevant risk registers are to be updated if risk accepted.

International Data Transfer Checklist

Before personal data can be transferred to an organisation outside of the United Kingdom it is necessary to carry out a preliminary investigation to determine the type of transfer being undertaken and the risks involved in making that transfer.

Please see the Guidance at Annex 1 for further information on how to complete this Checklist.

Please complete Parts A – C to the extent possible and return the completed Checklist to the Information Governance team at **dpa@abdn.ac.uk**

Part A: Background

This intended data transfer is between the University of Aberdeen and the other Organisation or Organisation(s) listed below.

Name of University/Organisation(s) involved in international transfer:	
Address and Name of Contact:	
Relevant Data Protection Laws in Country (if known):	
Description of Project or Contract:	
Is the Organisation a controller; joint controller or processor?	
How is the data being sent/shared/accessed?	
How long can the Organisation access the data (and any other Organisations/sub processor) and how long will it be held for?	
What technical and organisational security measures does the Organisation have in place to protect the data (to the extent known)?	
Will the Organisation forward the data to another Organisation or sub processor including for hosting purposes? If so, who and where will the data be held?	
Does this involve the use of the Grampian Data Safe Haven (DaSH)?	

The intended data flow is as follows:

	Data Item	Data Exporter ie sender	Data Importer ie receiver	Data Owner	Is this Sensitive Data (Yes/No)?
Example	Student ID No:	University of Aberdeen	SCNU	Student Records	No
1.					
2.					

3.					
4.					

Part B: Process for Assessing International Data Transfer

Question 1. Is a restricted transfer of data being undertaken?	**Yes**	**No**
a) Does the data comprise of personal data including pseudonymised data and is it necessary for this to be transferred? If data can be anonymised then it should be or if the transfer of personal data is not necessary then it must not be transferred.		
b) Is the data being transferred to a country outside of the United Kingdom		

If the answer to both Q1a) and b) is **YES** then a **Restricted Transfer** is taking place. Please move to Q2. If the answer is NO to either or both then please complete PART C and return the Checklist to: dpa@abdn.ac.uk.

Question 2. Is there an Adequacy Decision in place?	**Yes**	**No**
Is there an Adequacy Decision in place covering the country which is transferring/receiving the data? Please see current list within the Guidance at Annex 1 and include the name of the country here:		

If the answer to Q2 is **YES** then please complete PART C and return the completed Checklist to: dpa@abdn.ac.uk and await confirmation that the transfer may proceed (further documentation may be required). If the answer is **NO** then a **Transfer Risk Assessment (TRA)** must be completed. Please complete PART C and return the completed form to: dpa@abdn.ac.uk and the Information Governance Team will complete the TRA. Your input and assistance may be required to enable the TRA to be completed and any further documentation.

PART C: Sign Off

Date of Checklist	
Checklist completed by	
Date of Review of Checklist (if applicable)	
DPO Comments (if applicable)	

Annex 1 – Guidance for completion of the Checklist

Part A: Background information on the Project/International Data Transfer

Please complete Part A of the Checklist as comprehensively as possible. You may not be able to answer all questions however please complete the Checklist to the extent possible. It is important that the types of personal data and the data flows are documented accurately. Please add further rows to the data flow table if required. If the full details are not yet known, please include as much detail as possible. The Checklist should be reviewed and updated as the project, partnership or proposal develops.

When transferring personal data, the University of Aberdeen is required to abide by the requirements of the UK General Data Protection Regulation, the Data Protection Act 2018; the Human Rights Act 1998 and the common law duty of confidentiality (the "Data Protection Legislation"). The University may also have to comply with other international data protection laws depending on the details of the data transfer. For example, if the personal data is processed in a country outwith the UK relating to students in that country, then it is likely that local data protection laws will apply to this data rather than the Data Protection Legislation.

Part B: Process for Assessing the International Data Transfer

This Part of the Checklist is split into 2 Questions. Please complete this Part taking into account the following Guidance:

Question 1: Assessing whether a restricted transfer (defined below) is taking place involving personal data and whether it is necessary

The Data Protection Legislation only applies to information from which living people can be **directly or indirectly identified including pseudonymised data**. It does not include information relating to companies; deceased individuals or anonymised data (albeit other laws such as the law of confidentiality may still apply).

The Data Protection Legislation primarily applies to controllers and processors located in the UK, with some exceptions. It restricts the transfer of personal data to a separate organisation located outside of the UK, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies. Individuals risk losing the protection of the Data Protection Legislation if their personal data is transferred outwith of the UK. A transfer of personal data to a separate organisation located outside of the UK is referred to as a "restricted transfer". These restrictions apply to all transfers, no matter the size of transfer, the method or how often you carry them out.

If it is not necessary to make the transfer then it should be avoided or if anonymised data can be used instead then this should be used.

In assessing whether a restricted transfer is taking place, the Information Commissioner's Office has clarified that, you must consider any onwards transfer of the personal data by the organisation receiving the data. For example, where the data is shared with a supplier in the UK however they use sub processors based in the US. You will need to consider the following scenarios;

- Where the organisation/supplier is based in the UK and utilises the services of sub processors outwith the UK, you need to carry out due diligence to ensure the supplier has an appropriate safeguard in place however the University is not required to enter into an International Data Transfer with the third party or carry out a Transfer Risk Assessment for example. This requirement falls to the supplier to complete alongside their sub processor.

- Where the supplier operates in both the UK and outwith the UK (for example, they have staff working in offices in the UK and in Australia), the requirement to put in place the appropriate safeguard falls on the University.

The Information Governance Team will be able to advise further in these scenarios.

Please complete Question 1 in the Checklist. If the answer to both Q1a) and b) is **YES** then a **Restricted Transfer** is taking place. Please move to Q2. If the answer is NO to either or both then please complete PART C and return the Checklist to: **dpa@abdn.ac.uk** and await confirmation that the transfer may proceed (further documentation may be required). Please note that if further documentation is required then the timescales for completing this must be taken into account.

Question 2: Is there an Adequacy Decision in place?

If the transfer is taking place to one of the countries listed below then the transfer may take place as there is an adequacy decision in place. Please note that this list may be subject to change and this must be considered in any risks assessment associated with the project or contract.

Adequate countries and territories

Andorra	Denmark	Isle of Man	Portugal
Argentina	Estonia	Italy	Romania
Austria	Faroe Islands	Japan (transfers to private sector organisations only)	Slovakia
Belgium	Finland	Jersey	Slovenia
Bulgaria	France	Latvia	Spain
		Liechtenstein	
Canada (transfers to commercial organisations only)	Germany	Lithuania	Sweden
	Gibraltar		
	Greece	Luxembourg	Switzerland
	Guernsey	Malta	The Republic of Korea (South Korea)
Croatia	Hungary	Netherlands	
	Iceland		
Cyprus	Ireland	New Zealand	Uruguay
		Norway	United States of America (for organisations signed up to Data Bridge only)*
Czech Republic	Israel	Poland	

- For transfers to the United States of America, please contact the Information Governance Team who will carry out a search to ensure the organisation has signed up to the UK Extension to the EU-US Data Privacy Framework

Please complete Question 2 in the Checklist. If the answer is **YES** then please complete PART C and return the completed form to: **dpa@abdn.ac.uk** and await confirmation that the transfer may proceed (further documentation may be required).

If the answer is **NO** then a **Transfer Risk Assessment (TRA)** must be completed. Therefore, please complete PART C and return the completed form to: dpa@abdn.ac.uk and the Information Governance Team will

complete the TRA. Your input and assistance may be required to enable the TRA to be completed and the risks in the TRA must be signed off by the appropriate School or Directorate.

Part C: Sign Off

Please arrange for this sign off section to be completed and then return the Checklist to: dpa@abdn.ac.uk. This completes the Checklist.

Annex 2 – Transfer Risk Assessment (TRA)

Step 1: Assessing the transfer

This Transfer Risk Assessment must be completed by the Information Governance Team only in accordance with the Guidance for TRAs however input and sign off is required by the relevant Directorate or School

Requirement		YES/NO – If NO, explain why below. If YES, please document evidence.
Does the transfer comply with the rest of UK GDPR?	Data Minimisation Privacy Notice Lawful basis Security Processor obligations (if applicable)	
Is the TRA tool suitable for your transfer risk assessment?	[redacted]	

If either of the answers above are **NO**, then the TRA is not suitable and you should move to Step 4. If the answer to both is **YES**, then please move to Step Two.

Step 2 (Part A):

Question:	**YES/NO/DON'T KNOW**
Are the contractual safeguards likely to be enforceable in the destination country?	
If YES, please document the reasons why, based on the factors listed in Table A within the Framework.	

If the answer is **YES**, then please move to Step 3. If the answer is **No** or **Don't Know**, then please move to Step Two (Part B).

Step 2 (Part B):

Question:	LOW/MEDIUM/HIGH
If you have concerns that the contractual safeguards may be undermined, what is the level of risk of harm to data subjects?	

If the risk of harm is LOW, please proceed to Step 3. If the risk is HIGH or MEDIUM, consider whether additional measures are required:

Question:	YES/NO (IF YES – state which ones)
Can additional steps and protections be introduced to reduce the risks?	

If additional steps and protections can be taken in accordance with the Guidance then please document these steps/protections and move to Step 3. If not, then move to Step 4.

Step 3: Is there appropriate protection for the data from third party access?

Question:	YES/NO/DON'T KNOW (If DON'T KNOW assume it is NO)
Is the destination country's regime similar enough to the UK in terms of regulating third party access to data (including surveillance)	

If the answer is YES then this completes the Transfer Risk Assessment. Please complete Step 5 and consider if further documentation is required in accordance with Annex 3. If the answer is NO or DON'T KNOW, consider the following:

Questions:	
How likely is third party access to the data (including surveillance)? Minimal or not? If Minimal then the transfer may proceed. If more than a minimal risk, consider the question below.	Minimal or not?
What is the risk of harm to the data subjects considering the circumstances of the transfer and the destination country's regime? If low risk then the transfer may take place. If enhanced risk, consider the question below.	Low or Enhanced Risk?
Are you able to take extra steps and protections to reduce the risk of harm to low? If so, please state these in adjacent box and the transfer may proceed. If not, move to Q4.	Steps to be taken:

The Transfer Risk Assessment is now complete. Please complete Step 5 and consider whether additional documentation is required in terms of Annex 3, for example, IDTAs or if an exception assessment is required (Step 4 below).

Step 4: Does an exception apply to the transfer?

Question. Does an exception apply to the transfer?	**YES/NO – If YES, specify exception**
Is there an Exception in place which applies to the data being transferred/received? If YES then:	

Upon completion of this Step 4, please proceed to Step 5 and consider whether additional documentation is required in accordance with Annex 3.

Step 5: Sign off - Transfer Risk Assessment

Date of Checklist	
Checklist completed by	
Date of Review of Checklist	
DPO Comments (including requirement for any additional documentation eg IDTAs	
Information Asset Owner/Project Sponsor (Signature and Date)	
Escalation of risk required and outcome (if applicable)	

Annex 3 – Other Information Governance Requirements

This Annex 3 must be completed by the Information Governance Team only

Please document whether the following has been completed (if required):

Name of Document	**Completed (Y/N)**
Data Sharing Agreement (or appropriate clauses in the contract)	
Data Processing Agreement (or appropriate clauses in the contract)	
International Data Transfer Agreement (IDTA) or other appropriate safeguard	
Data Protection Impact Assessment	
Privacy Notices (new or updated)	
Other *(please specify)*	

Is the University of Aberdeen required to appoint a Data Protection Officer in the destination country? Y/N

Does the Record of Processing Activities require to be updated? Y/N

Completed By:	
Date:	

Approval/Review History

Version	Date	Action
1.0	Prepared by Data Protection Officer, 17 May 2022	Approved IGC, 1 June 2022
1.1	Updated by the Data Protection Officer following comments from the International Advisory Group, 20 June 2022	
2.0	Updated by DPO to reflect ICO guidance on International Data Transfers and UK adequacy decision, 14 February 2023	
3.0	Updated by DPO to reflect UK-US Data Bridge and include adequate countries, 06 November 2023	