Transfer Impact Assessment Template

Document Control	
Date of Assessment	
Author	
Reviewed By	
Review Date	*Ideally on at least an annual review cadence.*

Decision Summary	
Importer Details	
Third Country Details	
Purpose of Transfer	
Can the Transfer Take Place?	
Decision Approved by	
DPO Approval	

Glossary of Terms	
Exporter	Data exporter is a controller or processor established in the EU (or UK) that transfers personal data to a data importer outside of the EU (or UK)
Importer	Data importer is a controller or processor established outside the EU (or UK) that receives personal data from a data exporter inside the EU (or UK)
Article 46 Transfer Mechanism	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 (notwithstanding existence of an Adequacy Agreement.) These safeguards are detailed in GDPR Article 46 and can include Standard Contractual Clauses, Binding Corporate Rules, Approved Codes of Conduct and others.
Adequacy Agreement	The European Commission (or the UK Government) has the power to determine, on the basis of article 45 of the GDPR, whether a country outside the EU (UK) offers an adequate level of data protection. This is known as an Adequacy Agreement.
Special Category Data	Article 9 of the GDPR defines Special Category Data as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Essentially Equivalent	Essentially Equivalent can be taken to mean 'sufficiently similar' to. It does not mean identical. In this context for example, the level of protection in a third country does not need to be identical to that under GDPR. But, it should be

	similar enough that the transfer does not undermine the protections of the GDPR.
Public Authorities	Public Authority means any government or other public administration, including public advisory bodies, at national, regional or local levels, or any natural or legal person performing public administrative functions under national law.

Notes on Completing the TIA

Some important points to consider when completing the TIA:

1. This TIA assumes you have a good understanding of your international transfers already. If you do not know what international transfers your organisation is engaged in then you should first map your transfers. This is often documented in a Record of Processing Activity.

2. This TIA can be used to assess international transfers of personal data from both the EU and the UK, although the UK data protection regime is in a period of flux and this may be subject to change.

3. This TIA makes suggestions relating to dividing the responsibility for completing the TIA between exporter and importer. This is best practice and is recommended by both the EDPB and in the draft ICO guidance, but it is not essential. It is ultimately the responsibility of the exporter to complete the TIA, and sections can be completed by any party. However the importer is likely to have a better understanding of the local legal regime in the destination country and so it may be easier to have the importer complete these sections.

4. The TIA contains guidance notes throughout to help you complete the assessment. These are in *blue highlights* - please delete from your final TIA!

5. A TIA is not the same as a full-blown adequacy agreement assessment that would be completed by the European Commission. The TIA may represent a challenge to many organisations so it does not need to be overly detailed in its answers, it can be a relatively high level assessment.

6. The TIA prompts you to consider more complex transfer environments, especially in regards to 'onward transfers' of data, meaning that a non-EU importer of data subsequently transfers the data on to another third country. Please follow the guidance in the TIA in these circumstances.

7. Don't forget the other GDPR requirements for the processing! A TIA is just one assessment that relates only and specifically to the international transfer of data. The processing in general still needs to be in compliance with GDPR and may require other assessment documents to be completed such as DPIA, LIA, etc.

8. Below you will find some example scenarios as guidance:

Scenario 1: internal transfers between a corporate entity in the EU and a same group corporate entity in a third country. Complete the TIA *only if the two entities are separate controllers*. Flows of data within the same controller (or processor) are not transfers, even if the receiving party within the entity is in a third country. It is important here to understand that careful analysis of controllership status should be applied to subsidiaries and intra-group transfers. Corporate subsidiaries and affiliates are often separate controllers - if this is the case, complete the TIA. Here, the company can be both the importer and the exporter.

Scenario 2: internal transfers between a corporate entity in the EU and same group corporate entities in multiple third countries. Taking into account the above, if a TIA is needed, complete the TIA noting that separate TIAs will be needed for each third country destination, although some parts of the TIA (context of the transfer for example) will be duplicate.

Scenario 3: you are an importer only. Although individual exporters may have their own TIAs that they wish you to complete, you may wish to get ahead of the curve by completing a TIA ahead of time **.** You can complete the whole TIA**,** but note that the exporter/controller will have final say on whether to use it or not.

Scenario 4: you are an importer and you transfer the same data onto another sub processor in another third country. Similar to above, but additionally you should complete a separate TIA for the onward transfer. Further details are provided below.

Part 1 - Context of the Transfer

To be completed by the data exporter

This section should be used to detail the particular circumstances and contexts of the transfer, and the details recorded here should be considered when assessing the risks the transfer might pose to the rights and freedoms of the data subjects that will be conducted later in the TIA.

Details of the importer and exporter	
Name of the Data Exporter	
Country/countries in which exporter is located	*For the purpose of the TIA, this will be the EU member states/states in which the exporter is established.*
Is the exporter a public or private organisation?	
Name of the Data Importer	
Is the importer a processor or joint-controller?	
Is the importer a public or private organisation?	
Is the importer subject to professional or other rules or codes of conduct?	*This will be dependent on the context of the transfer. Professional rules or codes of conduct might apply for example to certain medical, legal, financial, etc. processes.*
Details of the transfer	

Which country is data being transferred to?	*This should be a single country. For data transfers to an importer based in multiple non-EU jurisdictions, a separate TIA should be completed for each country that data is transferred to.*
Is this a country with an EU Commission Adequacy Agreement?	*If yes, it is not necessary to complete the TIA.*
What is the purpose of the processing activity for which data is transferred?	
Will the transfer be systematic or on an as-needed/ad hoc/one-off basis?	
Categories of data subject	*ie. customer, client, patient, employee, etc.*
Categories of personal data transferred	*ie. name, address, ID number, etc.*
Is Special Category Data transferred?	
Is data relating to children transferred?	
Are any other sensitive data types transferred?	*Non-special category data types that are still potentially sensitive, such as financial information, bank account details, etc.*
How will data be transferred?	*Describe the technical means of the data transfer.*
Will data be stored by the importer or will the importer only access data via remote access to data stored in EU/EEA/UK?	
If stored, for how long?	
Could the purpose of processing be achieved without such a transfer?	*Consider whether the transfer is necessary or whether the purpose of the processing can be achieved without transferring data outside of the EU.*
What is the GDPR Article 46 Transfer Mechanism in place for the transfer?	*ie. SCCs, BCRs, certification, ad hoc contract, code of conduct*

Part 2 - Onward Transfers

To be completed by the data importer

International Transfers can be complex. On some occasions data may be transferred to a third country, and then subsequently transferred again to another third country. It is important that all international transfers are appropriately assessed and that transfers to sub-processors in other third countries are not forgotten about. This section should be used to document any such onward transfers.

Details of onward transfers	
Is data transferred to sub-processor(s) or third-parties based in other third countries outside of the UK/EU/EEA?	*If not, this section does not need to be completed.*
What is the purpose of the onward transfer?	
Countries in which sub-processors are located?	
Are these countries with an EU Commission Adequacy Agreement?	*If no, then a separate TIA should be completed by the Data Importer for each country and appended to this TIA.*
Could the purpose for the onward transfer be achieved without transferring personal data to the sub-processor(s) or other third-parties?	
List the countries for which subsequent TIAs will be completed	

Part 3 - Assessing the legal environment of the third country

To be completed by the data importer and/or data exporter

This section prompts you to assess the legal regime in the third country, in general terms and related to privacy law specifically.

The purpose here is twofold. Firstly, we essentially need to assess whether the Standard Contractual Clauses (or other export mechanism) can be enforced, if necessary, in the third country, by either the exporter or the data subjects (who are a third party beneficiary of the SCC.)

This means that we should consider whether both exporter and data subject have access to enforceable and effective legal remedies in the third country.

For example, if the third country has no effective rule of law then it is difficult to envisage a data subject being able to bring effective action against the importer to enforce their rights.

Secondly, we need to assess whether the SCC (or other export mechanism) will be able to offer protections that are 'essentially equivalent' to those that would be in place for data being processed only in the EU.

In order to answer these questions, we must consider the legal regime in the third country in general terms and related to privacy law specifically to come to a reasonable assessment.

The exporter should complete the determination fields at the end of this section.

We will return to these assessments at the end of the TIA.

Rule of Law and legal environment	
Describe the rule of law in the third country, in general terms	*This can be a high level overview. You should be able to draw on NGO reports, government papers, and media articles to develop an understanding of the state of the rule of law in the third country.* *Some important factors to consider:* ● *Independence of the judiciary* ● *Independence of judicial process* ● *Access to justice via court systems*

	Cite references to back up your assessment. *You do not need to be exhaustive!*
Describe the country's approach to human rights	*Again, this can be a high level overview. You should be able to draw on NGO reports, government papers, and media articles to develop an understanding of the state of human rights in the third country.* *Cite references to back up your assessment.* *You do not need to be exhaustive!*
Are foreign judgments or arbitration awards recognised or fairly enforced?	*One way to determine this is to assess whether the third country is party to conventions for recognition of enforcement of foreign judgments or arbitration awards (such as the Brussels Convention/the Hague Choice of Court Convention.)*
Privacy Legislation	
Does the country have a privacy law?	*Describe the privacy law in the third country. You may wish to consider the following aspects of the law:* ● *Does the privacy law have foundational principles?* ● *Does the law contain lawful bases under which data must be processed?* ● *Does the law have data minimization requirements?* ● *Does the law mandate personal data accuracy?* ● *Does the law require that data is processed securely?* ● *Does the law grant individuals with rights and freedoms concerning use of their personal data?* ● *Does the law contain provisions for the processing of sensitive data types?* ● *Does the law contain obligations relating to automated decision making and profiling?* ● *Is there an independent and effective supervisory authority?* ● *Does the supervisory authority have tools (enforcement action) to encourage compliance?*

Other Legislation?	
Are there any other legislations in the third country that are relevant to the processing context?	*For example, there may be other legislation relating to different data contexts, such as medical data, criminal record data, financial data, etc.*
Describe other legislation impacts on the data transfer	
Summary of findings	
If relying on Standard Contractual Clauses, will these be enforceable in the third country?	*Using the information recorded above, come to a balanced and reasonable assessment on whether you believe that the SCC will be enforceable in the third country legal system.*
Does the rule of law in the third country and the local privacy law offer 'essentially equivalent protections' as the GDPR?	*Again, based on the above information, come to a balanced and reasonable assessment on whether you believe that the transfer to the third country (with the SCCs in place) will offer an essentially equivalent protection as under GDPR.* *The level of protection in the third country does not need to be identical to that under GDPR. But, it should be similar enough that the transfer does not undermine the protections of the GDPR.*

Part 4 - Assessing the nature of state surveillance and public authority data processing in the third country

To be completed by the data importer

This section prompts you to assess the legal regime in the third country, with specific regard to the possibility of access to data by public authorities.

The process here is again twofold.

Firstly, we need to assess whether the third country offers safeguards and protections that govern public authority access to personal data, and again whether these are 'essentially equivalent' to those in the EU.

If you find that the third country does not have appropriate safeguards and protections that govern public authority access to personal data, then you should consider the likelihood of this occurring, given the context of the transfer, and the possible impacts on the data subject.

Processing by Public Authorities	
Are public authorities (military, defense, national security, criminal, other) able to access transferred data?	*You should be able to draw on NGO reports, government papers, and media articles to develop an understanding of the public authority's access to data.*
Describe the legal framework that controls state/public authority access to personal data?	*List the surveillance laws which apply to the Data Importer based on which public authorities may request access to the personal data*
Is this legal framework based on the rule of law and governed by clear, proportionate and necessary legal rules?	
Do individuals have fair redress to data processed by public authorities?	

Does an independent and impartial oversight system exist to oversee public authorities' access to personal data?	
Do public authorities publish transparency information about surveillance and data access?	
How is data sharing between public authorities governed?	
Is the Data Importer required by law to implement surveillance measures / intercept capabilities for personal data?	
Is the Data Importer legally entitled to challenge/object to requests for access to personal data from public authorities?	
Has the Data Importer ever received any requests from public authorities for access or disclosure of EU personal data?	
If yes, how many requests have been received in the past 5 years?	
For transfers to the US only *The below should be completed only for transfers to importers based in the US.*	
Is the Data Importer subject to the following Surveillance Laws: Section 702 FISA (50 U.S.C. § 1881a) Executive Order 12333 including any potential intelligence-sharing agreements with foreign governments and international organisations based thereon	

Presidential Policy Directive 28 (PPD-28)	
Has the importer ever received a subpoena from a US governmental authority related to the data being shared?	
Summary of findings	
Does the third country offer 'essentially equivalent protections' as the GDPR in relation to access to data by public authorities?	*Using the information recorded above, come to a balanced and reasonable assessment on whether you believe that there is appropriate governance of public authority data access in the third country that is similar to that in the EU.*
How likely is public authority access to the transferred data?	*Using the information above, assess the likelihood of access to data, given the context of the transfer:* *Remote, Low, Moderate, High*

Part 5 - Assessing the Transfer and Supplementary Measures

To be completed by the data exporter

Assessing the Transfer	
a. If relying on Standard Contractual Clauses, will these be enforceable in the third country?	*Take the answer at the end of Part 3 and Summarise as Yes/No*
b. Does the rule of law in the third country and the local privacy law offer 'essentially equivalent protections' as the GDPR?	*Take the answer at the end of Part 3 and Summarise as Yes/No*
c. Does the third country offer 'essentially equivalent protections' as the GDPR in relation to access to data by public authorities?	*Take the answer at the end of Part 4 and Summarise as Yes/No*
d. What are the likely risks to data subjects arising from the specific circumstances of the transfer? What is the risk rating?	*Consider :* • *Risks due to legal environment* • *Risks due to data types/data subject types etc* • *Risks due to public authority access to data* *Determine an overall Risk Rating:* *Remote, Low, Moderate, High*
YES to ALL of A, B, and C; OR NO to A, B, or C + risk (D) is REMOTE or LOW	**Make the Transfer**
Otherwise	**Put in place Supplementary Measures**

Supplementary Measures

If you need to put in place supplementary measures, these should be relevant and proportionate to the risks identified above.

The supplementary measures will vary depending on the nature and context of the transfer.

Technical Supplementary Measures:	*Some examples of Technical Measures:* • *Stringent Access Controls* • *Encryption* • *Pseudonymisation*
Contractual Supplementary Measures:	*Some examples of Contractual Measures:* • *Contractual Audit Requirement* • *Contractual requirement to send public authority access requests to the exporter*
Organisational Supplementary Measures:	*Some examples of Organisational Measures:* • *Limit importer processing activities* • *Mandate training functions* • *Limit importer access to data*

Repeat the Assessing the Transfer process taking into consideration the Supplementary Measures

a. If relying on Standard Contractual Clauses, will these be enforceable in the third country?	*Take the answer at the end of Part 3 and Summarise as Yes/No but taking into account the new supplementary measures*
b. Does the rule of law in the third country and the local privacy law offer 'essentially equivalent protections' as the GDPR?	*Take the answer at the end of Part 3 and Summarise as Yes/No but taking into account the new supplementary measures*

c. Does the third country offer 'essentially equivalent protections' as the GDPR in relation to access to data by public authorities?	*Take the answer at the end of Part 4 and Summarise as Yes/No but taking into account the new supplementary measures*
d. What are the likely risks to data subjects arising from the specific circumstances of the transfer? What is the risk rating?	*Consider :* • *Risks due to legal environment* • *Risks due to data types/data subject types, etc.* • *Risks due to public authority access to data* • *The new supplementary measures* *Determine an overall Risk Rating:* *Remote, Low, Moderate, High*
YES to ALL of A, B, and C; OR NO to A, B, or C + risk (D) is REMOTE or LOW	**Make the Transfer**
Otherwise	**Cease Transfer**