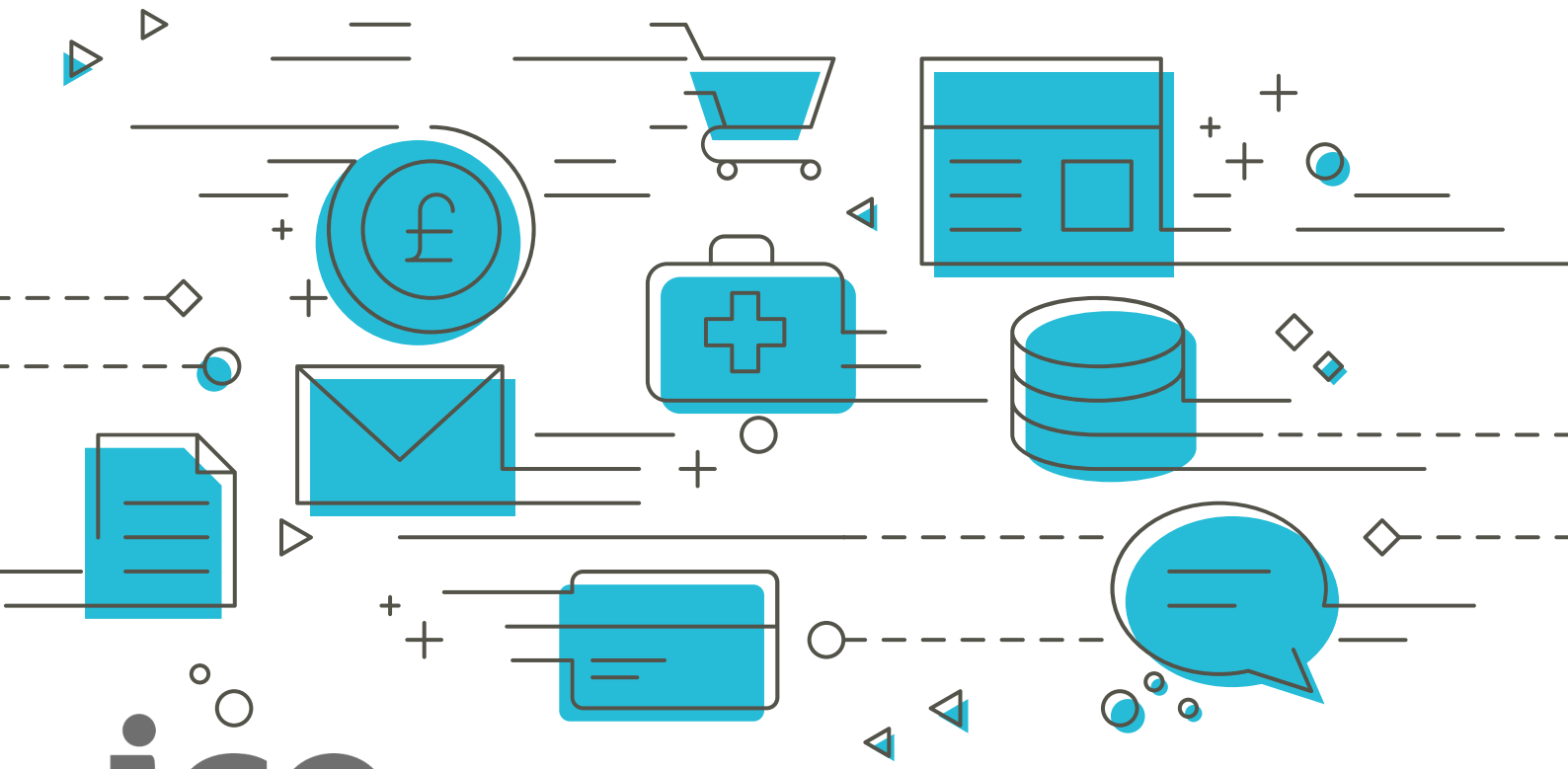
ICO consultation

Draft International transfer risk assessment and tool

August 2021



Information Commissioner's Office

Contents (for web navigation bar)

About this guidance 3
What is a transfer risk assessment (TRA)? 5
When should I carry out a TRA? 7
What is this TRA tool? 8
Roadmap: How do I use this assessment tool? 10
The transfer risk tool 11
Step one: Assessing the transfer 11
Step two: Is the IDTA likely to be enforceable in the destination country? 16
Table A: The enforceability of contractual safeguards in the destination country 17
Table B: Assessing overall risks to data subjects arising from the specific circumstances of the transfer, caused by concerns over the enforceability of the IDTA 20
Table C: Types and levels of measures to supplement the IDTA safeguards 26
Step three: Is there appropriate protection for the data from third-party access? 29
Table D: Assessing the third-party access or surveillance regime 32
Table E: Assessing the likelihood of third party access or surveillance 37
Table F: Assessing overall risk of harm to data subjects arising from the specific circumstances of the transfer caused by third party access 40
Table G: Types and levels of measures to supplement IDTA safeguards 44

About this guidance

Understanding and assessing risk is embedded into UK GDPR: when a Controller decides what measures to put in place to comply with UK GDPR, it must take into account "the risks of varying likelihood and severity for the rights and freedoms of natural persons" (Art 24). The Schrems II judgment embedded risk assessments into the rules on international data transfers. The Court held that before you may rely on an Article 46 UK GDPR transfer tool to make an international data transfer, you must carry out a risk assessment, and this is therefore a requirement under UK data protection laws. This risk assessment considers the risk of the transfer tool you put in place, not providing the right level of protection in the particular circumstances of that transfer, including the legal regime of the destination country.

This is not the same as the wholescale review the Government undertakes before making adequacy regulations for transfers to (for example) a country, looking at whether the level of data protection in that country as a whole is 'essentially equivalent' to the UK.

Every country has different laws and practices and we respect and welcome that diversity. Your transfer risk assessment should not look at whether the laws and practices in the destination country are identical to the UK. Rather, your focus should be on whether we share certain key principles which underpin our laws and practices, such as a respect for the rule of law.

This guidance focusses on two key aspects of the laws and practices of the destination country. First, whether the IDTA will be enforceable in that country, as this goes to the heart of what it means to put in place contractual protections.

Second we consider the destination country's regime which might require that the importer gives a third party access to the data you are transferring. This was the focus of the Schrems judgment, as it is a key point when local laws might conflict with the IDTA protections. It covers a range of circumstances, such as a Court Order requiring that the importer provides a copy of data to a private or public organisation and surveillance by private and public sector organisations.

Allowing third party access, including surveillance, is an important part of the checks and balances and protections in a country. It is one of the ways that we recognise the balance that has to be struck between fundamental rights (such as privacy and freedom of expression) both against each other and against the wider needs of society. Countries have significant discretion in how they balance these rights. Indeed, it may be more concerning if a destination country's regime does not have laws and practices for third party access, including surveillance, as this may mean that it happens without safeguards.

In your TRA the focus is not whether third party access, including surveillance, is permitted by local law, but rather whether the laws and practices include safeguards which are sufficiently similar in their objectives to the principles which underpin UK laws.

The ICO recognises that 'transfer risk assessments' can be a complicated exercise for organisations, particularly for those with limited resources. The importance of personal data flows to the economy is also recognised. The ICO has therefore committed to providing guidance and tools to enable organisations to comply with the law and continue to enable data flows.

This guidance has been written to give some general advice on how to carry out these transfer risk assessments, alongside tables you can use to help decide on the risk level when you are using the new ICO model international data transfer agreement(s) (IDTA) for routine transfers.

This guidance is relevant to you if:

- You are making a "restricted transfer" of personal data; and
- You are using the ICO's UK-specific standard contractual clauses for restricted transfers. We call these the ICO's model international data transfer agreement(s) (IDTA).

This guidance is relevant if you are using one of the other "appropriate safeguards" set out in UK GDPR Article 46, such as BCRs, although the TRA Tool is designed for the IDTA and has been published alongside it.

We consider that a data transfer is a "restricted transfer" if:

- [the UK GDPR applies to the personal data you are transferring;
- You (the data exporter) are sending data or making it accessible to a data receiver/importer to whom the UK GDPR does not apply; and
- the importer is a separate company or individual (including another company in the same corporate group).][1]

UK GDPR explains the circumstances when you are allowed to make a restricted transfer. One option is to rely on one of the "appropriate safeguards" set out in UK GDPR Article 46, which includes the IDTA.

The IDTA cannot provide safeguards for all risks in all counties. Therefore, before you can rely on an IDTA, you must also do a transfer risk assessment (TRA) which considers all the circumstances of the restricted transfer and checks if the IDTA provides appropriate safeguards for your restricted transfer.

This guidance includes a TRA tool to help you to both use IDTAs and to demonstrate your compliance with the requirement to carry out a TRA (as

[1] Note: this is our current guidance, but see Consultation Question 6 regarding whether we should update our interpretation of a restricted transfer.

required by the accountability principle of UK GDPR). You can also use the decision trees within the TRA if you are planning to make a restricted transfer of personal data using Binding Corporate Rules (BCRs) or another article 46 transfer tool.

There are other ways in which you may carry out a TRA, this TRA Tool is just one approach. The important point is that you have satisfied yourself that the IDTA (or other Article 46 transfer tool) provides appropriate safeguards in the context of your particular transfer. You will make a binding promise that you have done this in the IDTA.

In line with our Regulatory Action Policy, if you can show that you have used your best efforts in completing a TRA, whether or not you use this TRA Tool, if it later turns out that your decisions were not correct, we will take this into account in our likely approach to any breach of Chapter V UK GDPR.

Further reading

We also produced guidance on International Transfers

Regulatory Action Policy

What is a transfer risk assessment (TRA)?

A transfer risk assessment (TRA) enables you to make a restricted transfer when you plan to rely on one of article 46 transfer tools, such as the IDTA. The TRA helps you ensure that the article 46 transfer tool provides appropriate safeguards in the particular circumstances of your restricted transfer.

We recognise that you may find this challenging. The TRA Tool set out below aims to guide you through the process when you are planning to use an IDTA for routine transfers.

The IDTA provides a baseline of appropriate safeguards for any regime which is sufficiently similar to the key standards which underpin the UK's legal regime, with particular regard to the enforceability of the IDTA and for managing the risks arising from third party access (including risks that may arise from surveillance). In your risk assessment you will check whether for your restricted transfer, taking into account all the circumstances of that restricted transfer, the IDTA provides protection for the data subjects, which is sufficiently similar to the **relevant** protections they have when their data is in the UK.

You do not need to look at the whole regime of the destination country, **only those parts of the destination country's regime which are relevant to your restricted transfer**.

Our words "sufficiently similar" come from a legal test of "essential equivalence" which requires a comparison between the level of protection to data subjects in the destination country with that in the UK.

The level of protection in the destination country does not need to be identical to that in the UK under UK GDPR. But, it should be sufficiently similar to its key underlying standards to ensure that the transfer does not undermine the protections of the UK GDPR which are relevant to that transfer.

In some cases it will be obvious that the regime of the destination country provides very similar protections to the relevant protections in the UK. For example, it respects the rule of law, you will be able to enforce the contract in the courts or in arbitration (either is fine) and there is robust regulation of third parties accessing the data (including surveillance).

In many others, it is not going to be so clear; there will be a range of factors for you to consider to find a proportionate balance between your interest in making the transfer and the privacy rights of individuals. In these cases we look to the Article 8 Right of Privacy in the European Convention of Human Rights, which the Human Rights Act 1998 incorporates into UK law. It helps us find the right balance between the different interests which are affected.

There are many relevant factors that you should take into account; you can break these down into three main groups:

First, the particular facts of your restricted transfer, including:

- the type of personal data transferred;
- categories of data subject;
- types of entities involved in the transfer;
- sector in which the transfer occurs;
- purpose of the transfer;
- format of the data;
- method of transfer;
- the technological and organisational security the importer has in place to protect the data;
- whether the data will be stored outside the UK or whether there is remote access to data stored within the UK;
- the movement of data when under the control of the importer, which countries will the data will be held in; and
- the possibility of data being forwarded on by the importer to another entity.

Second, the particular facts about the destination country, including:

- whether there are **partial** UK adequacy regulations in relation to that country;
- its human rights record

- its legal and court system, and how close that it is to the UK legal and court system
- how overseas judgments are recognised and enforced; and
- its laws and practices regulating third parties access (including public authority surveillance).

Third, the potential impact on the data subjects of the transfer, and any risk of harm to data subjects you identify.

The aim of your TRA is to enable you to decide whether the IDTA on its own provides appropriate safeguards for your restricted transfer, or whether you will need to take extra steps and protections. There may be some situations where, even with extra steps and protections, the IDTA is unlikely to provide appropriate safeguards. In that case you may need to consider another Article 46 transfer tool or one of the exceptions.

Our guidance as to when the level of risk means the IDTA will provide appropriate safeguards is set out in the TRA tool (the section "Roadmap: How do I use this assessment tool?" provides a useful overview).

Where your IDTA covers repeated transfers of personal data or an ongoing flow of data to your importer, you must regularly reassess the level of protection the IDTA provides (and any extra steps and protections you took alongside the IDTA). You must ensure that the level of protection does not decrease over time. You need to consider whether the level of protection is undermined by:

- changes to the processing by the importer;
- changes to the legal framework in the destination country; or
- technical developments facilitating the by-passing of security arrangements.

When should I carry out a TRA?

You will need to carry out a TRA if you are making a restricted transfer and you wish to rely on one of article 46 transfer tools, such as the IDTA. The TRA helps you ensure that the article 46 transfer tool provides appropriate safeguards in the particular circumstances of your restricted transfer.

You do not need to carry out a TRA if you are making a restricted transfer to any country covered by UK adequacy regulations or if the restricted transfer is covered by one of the exceptions.

If you know that the importer will be sending on the data to third parties you will need to look at how this complies with the IDTA. If the importer will put in place an agreement which maintains the level of protection of the IDTA or uses another Art 46 transfer tool, then either you or the importer must make sure there is a TRA which covers that onward transfer of data.

Where you are making a series of connected transfers, you can carry out one TRA which covers all of them.

Further reading

We have produced guidance on international transfers

Relevant provisions in the legislation

See UK GDPR Article 45 and Recitals 103-107 and 169 and UK GDPR Article 49 and Recitals 111-112

What is this TRA tool?

There are many ways to conduct a TRA, and this TRA tool is just one method. It is designed to assist you when making **routine restricted transfers** (rather than the more complex transfers referred to in the next paragraph). The TRA tool consists of three steps. It provides a structured list of questions to work through and tables to help you assess risk at each step.

The tables set out key indicators in relation to the laws and practices in the destination country and factors relating to the data you are transferring, and link these to risk levels. We have tried to choose indicators which are relatively straightforward for you to identify, perhaps with the assistance of the importer. This is a broad approach, which is why it can only be used for those transfers which are not complex or high risk.

You will need to do more detailed risk assessment for transfers which are complex (for example, the importer is based in more than one country) or involve a high risk (for example, where you need to complete a data protection impact assessment (DPIA)). You can still use the decision tree contained in this TRA tool, if you find it helpful, but you do not need to do so.

In certain cases, the TRA tool may indicate that it is unlikely you can proceed with your proposed transfer. In these cases, you may consider completing a more detailed risk assessment or relying on another appropriate safeguard or an exception. You may wish to seek professional advice to help you understand your options.

The laws and practices of the destination country

In this TRA tool we ask you to consider the laws and practices of the destination country. The "**destination country**" is the country where the importer is based; think about which country's laws will directly apply to the importer when it receives the data.

We know that it may be difficult for you to form a detailed understanding of the risks associated with the legal framework in the destination country. However, you may be able to make an initial assessment of its legal and political landscape with information you can find from publicly available sources, including reports issued by the Foreign Commonwealth and Development Office and charitable organisations. You may be able to refine your assessment with information your importer provides on the local laws and practice. This may provide enough information for you to use this TRA tool for routine international transfers.

If you are unable to form an assessment of the legal framework in the destination country, you may need to obtain expert advice. Alternatively, you may use this TRA tool on the assumption that the legal regime in the destination country does not provide similar protections to the UK. As we explain in step three of the TRA tool, in some circumstances you may be able to go ahead with the transfer even making this assumption. In these circumstances, you do not need to carry out a more detailed assessment of the legal regime in the destination country.

Low risk of harm to data subjects

At certain stages in the TRA tool, we ask you to assess the risk of harm the transfer causes to data subjects. You may proceed where there is either no or a low risk.

What we mean by a "**low risk of harm**" is that:

- there is more than a minimal risk of the relevant event occurring which may infringe data subject rights; and
- even if that relevant event does happen, the impact on data subjects would not cause them significant harm.

The TRA tool provides guidance to assist you in your decision making. It is, however, your responsibility to assess whether appropriate safeguards are in place to protect the rights of data subjects.

Example

Further reading

Human Rights Act 1998 Article 8 (1) and (2):

In more detail – ICO guidance

We have produced guidance on International Transfers and on DPIAs

Roadmap: How do I use this assessment tool?

The tool has three steps to help you carry out your risk assessment in a logical and structured way. We give guidance at each step to help you assess whether you can proceed with the transfer. We provide the tables to help you make your risk assessment.

Step one: Assessing the transfer

You confirm that this tool is suitable for your restricted transfer. You confirm that the restricted transfer meets other UK GDPR obligations (it may not be if the transfer involves a high risk to data subjects). You then assess and record the nature of the restricted transfer.

Step two: Is the IDTA likely to be enforceable in the destination country?

You assess whether the IDTA is enforceable in the destination country. If you consider that it is likely to be enforceable you move to step three.

Where you have concerns about the IDTA's enforceability, you carry out a supplementary risk assessment to assess whether this gives rise to a risk of harm to data subjects and whether any extra steps or protections could reduce the risk.

If you assess there to be no or a low risk of harm, you can proceed to step three. If you assess there to be an enhanced risk of harm, you should not continue using the TRA tool for your risk assessment.

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

You assess the destination country's regime for regulating third-party access to personal data (including surveillance).

At the end of step three, you can go ahead with your transfer if:

- the destination country's regime for regulating third-party data access (including surveillance) is sufficiently similar to principles which underpin the UK regime; or
- the possibility of third-party access (including surveillance) is minimal regardless of the destination country's regime; or

- the risk of harm to data subjects is low, even if third-party access (including surveillance) did take place.

Example

The transfer risk tool

Step one: Assessing the transfer

Decision tree	
Does the transfer comply with the rest of the UK GDPR?	
Yes ↓	No **TRA tool not suitable**
Is this TRA tool suitable for your transfer risk assessment?	
Yes ↓	No **TRA tool not suitable**
Record the specific circumstances of the transfer	
↓ **Go to Step 2**	

Can you satisfy the key requirements under the UK GDPR?

This TRA focuses on the international transfer rules. However, you should not make the restricted transfer without ensuring that it meets the rest of the UK GDPR requirements.

Making a restricted transfer constitutes processing of personal data. Like all processing, you must satisfy the fundamental principles set out in Article 5 UK GDPR. If your processing does not meet those requirements then the restricted transfer cannot go ahead (and you do not need to even ask the question whether your restricted transfer meets the specific requirements which apply to restricted transfers).

For example, you should check the arrangements meet the following key requirements:

- **Data minimisation** – is the data you are proposing to transfer **adequate, relevant and limited to what is necessary**?
- **Security** – have you put in place **technical and organisational measures to ensure a level of security appropriate to the risk**? Does this take into account any particular risks in the countries where the data is going?
- **Lawful basis** – is the transfer of data **fair and lawful**, and is there a lawful basis to transfer the data? Thinking about the importer's **purpose** for which it will be using the data:
    - If the importer is your Processor or Sub Processor, does the purpose of the restricted transfer fall within your purposes for processing the personal data?
    - Otherwise, if the importer was in the UK, would it comply with Art 6 lawfulness of processing and (if there is any special category data or criminal records) Articles 9 and 10? If not, does this make the transfer unfair?
- **Processor obligations** – if the importer is a processor, have you put in place a processor contract?
- **Transparency** – have you made data subjects aware through appropriate privacy notices of the processing that is taking place?

Further reading – ICO guidance

We have produced guidance on accountability and principles

Is this TRA tool suitable for the proposed transfer?

The TRA is suitable when using the IDTA to make a routine transfer of personal data to an importer based in a country outside of the UK.

The TRA is **not suitable** if:

- the proposed restricted transfer does not satisfy the key requirements set out above;
- the proposed restricted transfer is to a country covered by UK adequacy regulations;
- you are relying on an exception to make the transfer; or
- the specific circumstances of the restricted transfer mean that it is **too high risk** or **too complex** for this tool. For example, if:
    - (other than UK law) more than one country's laws apply to the importer's processing of the data, for example because the data will be handled by the importer and its branches in other countries. (This is not the same as the importer forwarding on data to other organisations, such as the importer's processors. In those cases, you need to check that the importer will be able to comply with the IDTA clauses about forwarding on data);
    - the transfer involves the use of new technologies, or the novel application of existing technologies;
    - the transfer requires a DPIA under UK GDPR; or
    - the transfer is to a destination country which has a human rights record which could produce a high risk for data subjects in the context of the specific transfer. There are many public sources which set out the human rights record for countries. For example, the Foreign, Commonwealth & Development Office (FCDO) produce regular Human Rights and Democracy Reports. If there are **partial** UK adequacy regulations for that country (which do not cover your restricted transfer), this is a strong indicator that the UK government considers that country to have a satisfactory human rights record.

If the TRA tool is not suitable for your risk assessment, you may still use the questions below as part of your risk assessment, although the tables would not be suitable for you to use. You may need to carry out a more detailed risk assessment or consider relying on another transfer mechanism or an exception. You may wish to seek professional advice.

Example

What are the specific circumstances of the restricted transfer?

It is important that you map out the data flows and record the **specific circumstances of the transfer**. You need this information in order to answer the questions below.

You must consider and document the following:

- Who is it going to? What kind of organisation is the importer? (eg a public regulator like the ICO, an IT company, a parent or service company in your group). Is the importer a controller, joint controller, processor or sub-processor?
- Where is the importer located? Will the importer be forwarding on the data to another organisation?
- Will the importer forward the data further to any other organisations and, if so, what kind of organisation are they and where are they located?
- Why are you making the transfer? What will the importer (and any other party to whom they forward on the data) be doing with the personal data?
- Who is the data about? Set out the categories of data subject (eg customers, employees or business contacts).
- What type(s) of data are you transferring, and does it include any special categories of personal data, or other more sensitive types of data such as financial transaction data, communications data, travel related data or confidential records?
- Is the importer subject to professional or other rules, which apply in addition to the general legal regime of the destination country? (eg if the importer is a law firm, then it may be subject to rules of professional conduct).
- What technological and organisational security measures will the importer have in place to protect the data?
- What is the format of the transferred data? For example, is it plain text, pseudonymised or encrypted?
- How are you sending the data? For example, are you transmitting it by email, website encryption or secure file transfer protocol (SFTP)? Or does it involve remoted access to data stored in the UK?
- For how long can the importer (and other recipients) access the data?
- How often will these transfers occur?
- How much personal data are you transferring?

In more detail – ICO guidance

We have produced guidance on controllers and processors and special category data

Further reading

We have produced guidance on international transfers

Relevant provisions in the legislation

See UK GDPR Article 45 and Recitals 103-107 and 169 and UK GDPR Article 49 and Recitals 111-112

Step two: Is the IDTA likely to be enforceable in the destination country?

In the first part of this step, you will assess the enforceability of the contractual safeguards that the IDTA provides in the destination country. If this satisfies you, you can move on to step three. If you have concerns,

you should carry out the extra steps and protections assessment that the second part of step two outlines.

<table>
<tr><th colspan="4">Decision tree</th></tr>
<tr><td colspan="4">Step 2A Are the contractual safeguards likely to be enforceable in the destination country?</td></tr>
<tr><td>Yes
↓</td><td colspan="2">Don’t know
↓
Assume serious concerns</td><td>No
↓</td></tr>
<tr><td rowspan="4">Go to Step 3</td><td colspan="3">Step 2B Taking into account the specific circumstances of the transfer and your concerns about the destination country regime, what is the risk of harm to individuals</td></tr>
<tr><td colspan="2">Low risk
↓</td><td colspan="2">Enhanced risk
↓</td></tr>
<tr><td colspan="2" rowspan="2">Go to Step 3</td><td colspan="2">Are you able to take extra steps and protections to reduce the risk of harm to low risk?</td></tr>
<tr><td>Yes
↓
Go to Step 3</td><td>No
↓
TRA tool not suitable</td></tr>
</table>

Step two A: Are the contractual safeguards enforceable in the destination country?

You need to assess whether the legal regime in the destination country is likely to respect the contractual safeguards the IDTA sets out, in a way that is sufficiently similar to how it would be enforced in the UK. This is to ensure that the level of protection the UK GDPR guarantees is not undermined and that enforceable data subject rights and effective legal remedies are available for the exporter and for data subjects.

What do I need to do?

Table A provides a guide as to the factors which impact the extent to which the legal regime in the destination country provides enforceable and effective rights to the data exporter and data subjects. You should look at the factors in the round to form a view of the destination country's legal regime. You could ask the importer for assistance with this.

Table A: The enforceability of contractual safeguards in the destination country

Factors suggesting there are enforceable rights and effective legal remedies	**Factors indicating areas of concern about enforceable rights and effective legal remedies**
• The country recognises the rule of law (ie there is an established and respected legal and court system)	• Evidence of lack of respect for the rule of law
• You can enforce foreign judgments or arbitration awards	• Foreign judgments or arbitration awards not recognised or fairly enforced

• The jurisdiction is party to a convention for recognition of enforcement of foreign judgments or arbitration awards. The key Conventions you might consider are:
  ○ the Brussels Convention; or
  ○ the Hague Choice of Court Convention
	• The jurisdiction is not party to international conventions for recognition of enforcement of foreign judgments or arbitration awards. The key Conventions you might consider are:
	  ○ the Brussels Convention; or
	  ○ the Hague Choice of Court Convention.

• There is ready access to justice through the court system which provides means for redress and effective remedies • The rights of third party beneficiaries under contracts are recognised and enforced	• Limited access to justice, especially for overseas litigants • Access to justice is possible, but it can be a lengthy process

Factors suggesting there are enforceable rights and effective legal remedies	Factors indicating areas of concern about enforceable rights and effective legal remedies
• High levels of integrity and independence in the judicial process	• Legal system has a limited degree of independence and impartiality • Evidence of significant or widespread levels of corruption
• There are **partial** UK adequacy regulations in relation to the country (which do not cover your restricted transfer). ○ This is a strong indicator of all the above factors, except you must still consider whether you can enforce foreign judgments and arbitration awards.	

Recording your findings

You should document your findings so that you have a record of how you reached your assessment.

Further reading:

We have produced guidance on documentation

Relevant provisions in the legislation

See UK GDPR Article 30 and recital 82

Decision point

If you decide that:

- the legal regime in the destination country supports the contractual rights and protections that the IDTA sets out, you should **proceed to step three**; or
- you have concerns that the contractual rights and protections guaranteed by the IDTA may be undermined, you should carry out a **supplementary risk assessment** as step two B describes below.

Example

Step two B: Supplementary risk assessment

If you have concerns about whether the IDTA is enforceable in the destination country, you can continue to Step three, if the risk of harm to data subjects, caused by those concerns, is low.

Consider:

- the level of **risk of harm** to data subjects as a result of the transfer in light of the concerns you have about the enforceability of the IDTA; and
- whether you can appropriately reduce such risk by applying any **extra steps and protections** *(include hyperlink to "extra steps and protections" guidance note – see below)* alongside the IDTA.

How do I assess the risk of harm?

To help you in assessing the **risk of harm** to the data subjects as a result of your concerns about the enforceability of the IDTA, you should look into the specific circumstances of the transfer. Some data sets carry greater potential for risk of harm than others.

You should therefore look at the particular risks attached to the data you are transferring, and whether there are factors which increase or decrease the risk of harm to data subjects if the IDTA is difficult to enforce against the Importer. This includes factors which make it more likely that the Importer would comply with the IDTA or a UK Court Order or Arbitration Award, without you or a data subject needing to bring legal action in the destination country.

Please consider whether this assessment would benefit from professional legal advice about the local laws of the destination country.

Table B provides a guide to help you do this. The Table references different risk levels (low, moderate and high) and factors which may reduce or increase that risk, to help you form an overall view of the potential harm.

Table B: Assessing **overall risks to data subjects** arising from the specific circumstances of the transfer, caused by concerns over the enforceability of the IDTA

Level of risk of harm to data subjects	**Low**	**Moderate**	**High**
The columns set out examples of certain categories of data subjects and relevant types of data. This list is not exhaustive, nor determinative. We intend it to help indicate the likely risk of harm to data subjects associated with particular transfers. It is important that you assess risk of harm in each case by referring to the context of the transfer's specific circumstances and the concerns about enforceability you have identified above.	**Staff**		
	Basic employment contact details, eg name, job title	Non-sensitive employment records, eg CV, payroll history	Special category employment records, eg sickness or absence records, health information, equality monitoring data, criminal records Sensitive information, eg banking details, passwords
	Members of the public or consumers		
	Basic contact information, eg shipping details, marketing preferences	Non-sensitive information, eg buying preferences, order history, basic credit scores	Special category records, eg order history for medication Sensitive information, eg payment or banking details, passwords

Level of risk of harm to data subjects	Low	Moderate	High
	Professionals, business contacts, suppliers		
	Basic contact information	Non-sensitive information, eg course of dealings, order history	Special category records, eg order history if that reveals special category data Sensitive information, eg payment or banking details, passwords
	Patients		
		Non-health-related personal data	Health or medical data

Adjustments to the level of risk of harm to data subjects	**Factors which may reduce or increase the risk of harm to data subjects**	
The following are circumstances which may increase or decrease the risk of harm to data subjects. This list is not exhaustive, nor determinative. It provides an indication of factors which may increase or decrease the risk	**REDUCE** 	**INCREASE** 
	• Data already in the public domain • Importer is a processor or sub processor of the Exporter, and the data subject could take legal action against the Exporter in most circumstances • The data subject has expressly confirmed that he has been informed of the potential risks of the transfer and has no concerns in relation to the same, and this has been documented. • There are **partial** UK adequacy regulations in relation to the destination country (which do not cover your restricted transfer).	• Data subjects are children or vulnerable adults • Risk of harm to additional individuals other than the data subjects (eg family members) • A large volume of data relating to an individual • Processing by importer includes automated decision making, including profiling, which produces legal effects or similarly significantly affects the data subject • If there was a problem, it is likely that you / a data subject would need to enforce the IDTA (or enforce a UK court order or arbitration award) in the destination country in order for the

Adjustments to the level of risk of harm to data subjects	**Factors which may reduce or increase the risk of harm to data subjects**	
		importer to comply.
The following are circumstances which may decrease the risk of the importer ignoring a UK court order or UK arbitration award (and so cause no harm to data subjects). This list is not exhaustive, nor determinative. It provides an indication of factors which may increase or decrease the risk	**REDUCE** 	
	• Importer and exporter are within the same group of companies • Importer is bound by professional codes of conduct (eg solicitors) • Importer is bound by regulatory obligations (eg financial services sector) • Importer is a reputable global company (eg an international bank or major cloud hosting service) • Importer has signed up to an ICO-approved code of conduct. • Importer has a certification under an ICO-approved scheme	
The overall risk to data subjects increases or decreases, depending on how similar the regime of the destination country is to the UK, for	 **Similarity to level of UK protection**	 **Divergence from level of UK protection**

Adjustments to the level of risk of harm to data subjects	Factors which may reduce or increase the risk of harm to data subjects	
supporting the contractual rights and protections in the IDTA. For example, if the destination country regime is similar to the UK (albeit with some concerns), you may decide that categories of data which are in the moderate risk box above, become low risk.		

Relevant provisions in the legislation

See UK GDPR Articles 40 and 42 (external link)

Further reading

We have produced guidance on codes of conduct, certification and special category data.

Extra steps and protections – what do I need to do?

Once you form a view on the potential risks, you should consider whether you could apply any **extra steps and protections** to safeguard the data and reduce the risks you identify.

Table C is a non-exhaustive list of typical extra steps and protections and guidance on how effective they may be at reducing the risk of harm to data subjects. These cover additional technical, organisational or contractual protections (above those already in the IDTA). Table C references different levels of risk reduction (basic, enhanced, significant) to help you form an overall view of the effectiveness of the measures.

You may need to change the IDTA (the Tables and TRA Extra Steps and Protections) to make sure the measures you use are a binding part of the IDTA.

Table C: Types and levels of **measures to supplement** the IDTA safeguards

Type of additional measures	**Basic**	**Enhanced**	**Significant**
Access controls *Either minimises likelihood of a breach of the IDTA occurring or reduces risk of harm to data subject if a breach of IDTA occurs*	You will password protect data prior to transfer to importer. You will provide the password separately where the Importer is to process the data beyond storing it.	You will encrypt the data prior to transfer using an appropriate encryption solution (i.e. storage encryption / encryption at-rest) and you will implement suitable key management procedures	You will encrypt the data prior to transfer using appropriate encryption solution and you split the encrypted datasets between multiple parties.
Changes to the data *Either minimises likelihood of a breach of the IDTA occurring or reduces risk of harm to data subject if a breach of IDTA occurs*	You review the purposes and scope of the transfer and further minimise the amount of personal data you transfer (ie only certain data fields), but it is not anonymised or pseudonymised	You apply pseudonymisation techniques to the data prior to transfer and the importer does not have access to the additional information.	You split pseudonymised datasets between multiple entities, so that there is a minimal risk that any on party could identify a data subject. Note: You should also consider anonymisation techniques. If the data is effectively anonymised in the hands of a receiver so that it is no longer personal data, the UK GDPR transfer restrictions will not

Type of additional measures	Basic	Enhanced	Significant
			apply
Contractual *Additional contract clauses in IDTA to reduce risk of Exporter or Data Subject being unable to enforce IDTA rights.*	Importer and/or exporter has an enhanced data subject complaints process, including compensation scheme.	If Exporter has sufficient financial resources: contractual right for data subject to bring a claim against the exporter if the importer fails to comply with UK court order or arbitration award.	If Exporter has sufficient financial resources: data subject can bring a claim against the exporter for any breach of IDTA by importer. Data subject can bring claim against a UK organisation in the same group as the importer (with sufficient financial resources) for breach by the importer. Confirmation and commitment to maintain: • Professional or regulatory status • ICO code of conduct • ICO certification

Further reading – ICO guidance

We have produced guidance on security, encryption and passwords, as well as draft guidance on anonymisation.

Recording your findings

You should document your overall findings, showing both your assessment of the potential risk of harm to the data subjects and the impact of applying any extra steps and protections. This should be sufficiently clear and detailed to provide a record of how you reach your assessment.

Further reading – ICO guidance

We have produced guidance on documentation.

Relevant provisions in the legislation

See UK GDPR Article 30 and Recital 82

Decision point:

If you decide that:

- there is either **no or a low risk of harm** to data subjects (taking into account any reduction you can make to the risk by applying extra steps and protections), you should **proceed to step three**; or
- there is an **enhanced risk of harm** to data subjects that you cannot appropriately reduce by extra steps and protections, **you should not continue using this TRA tool for your risk assessment**. Instead, you should do a more detailed risk assessment or consider relying on an exception. You may consider seeking professional advice before proceeding further.

Example

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

In step three you assess the destination country's regime for regulating third-party data access, including surveillance.

<table>
<tr><th colspan="5">Decision tree</th></tr>
<tr><td colspan="5">Is the destination country's regime similar enough to the UK's regime in terms of regulating third party access to data (including surveillance)?</td></tr>
<tr><td>Yes
↓</td><td colspan="2">Don't know
↓
Assume serious concerns</td><td colspan="2">No
↓</td></tr>
<tr><td rowspan="6">Make the transfer</td><td colspan="4">How likely is third party access to the data (including surveillance)?</td></tr>
<tr><td>Minimal risk
↓
Make the transfer</td><td colspan="2">Don't know
↓
Assume more than a minimal risk
↓</td><td>More than a minimal risk
↓</td></tr>
<tr><td colspan="3">Considering the circumstances of the transfer and the destination country's regime, what is the risk of harm to data subjects?</td></tr>
<tr><td rowspan="3">Low risk
↓
Make the transfer</td><td colspan="2">Enhanced risk
↓</td></tr>
<tr><td colspan="2">Are you able to take extra steps and protections to reduce the risk of harm to low risk?</td></tr>
<tr><td>Yes
↓
Make the transfer</td><td>No
↓
TRA tool not suitable</td></tr>
</table>

In Step three you may need to assess the destination country's regime for managing when access to data by third parties (including surveillance) can be required and the safeguards for individuals. You do not need to do this assessment (and can continue with this TRA tool and proceed with your transfer) if you are satisfied that, given the circumstances of the transfer and the nature of the personal data:

- the possibility of third-party access, including surveillance, is minimal; or
- if third-party access, including surveillance, did take place, the risk of harm to data subjects is low.

How do I assess the destination country's regime for regulating third party access to data (including surveillance)?

Consider whether the destination country provides legal safeguards for data subjects when the law requires that third parties (including public authorities) are able to access their data, and whether those legal safeguards are sufficiently similar to the UK's underlying standards.

Below, when we say third party access is "**concerning**" we mean that you have significant or substantive concerns whether that particular type of third party access or surveillance, is subject to standards that are not sufficiently similar to those that underpin the UK's regime.

We recognise that this is a complicated exercise for organisations, particularly for those with limited resources; we don't expect you to become experts in international surveillance regimes. If you are not able to form a view of the risk in relation to the destination country's approach to third party access (including surveillance), you can go straight to the question "What is the likelihood of third-party access to the data (including surveillance)?", on the basis that the third party access regime in the destination country may be concerning.

What do I need to do?

Table D provides a guide to factors you should consider to help form a view as to the extent to which the third party access (including surveillance) regime in the destination country is likely to safeguard the rights of data subjects.

These are key indicators which will give you an overview of the risk in relation to the destination country's approach to third party access (including surveillance). All the key indicators do not need to apply; you should look at these factors in the round to form a view of the destination country's legal regime. You may wish to seek assistance with this from the importer.

Looking at the factors you may have only have concerns about some specific types of third party access (including surveillance) which occur in the destination

country. For the purpose of this TRA Tool, you can then focus on that **concerning** third party access for the following steps.

Once you have made your assessment, consider whether it would be appropriate to obtain approval of your assessment by a qualified legal professional.

Table D: Assessing the third-party access or surveillance regime

Factors that are likely to safeguard the rights of data subjects	**Factors that are likely to undermine the rights of data subjects**
Whether there are laws which set out when and how the law can require access to data is given to third parties including public authorities	
Public authorities have powers to access data from private companies, including to intercept communications, with meaningful safeguards. For example, public authorities cannot use these powers without a court order or warrant.	Public authorities have wide powers to intercept communications and to access data from private companies, with few, if any safeguards. Requests for information by law enforcement and other public authorities from private sector companies are at an unexpected and disproportionate level.
There are rules setting out when private companies are able to obtain access to data. For example, by Court Order.	There is general and indiscriminate sharing of information between private companies, which is unregulated.
Organisations can undertake workplace monitoring, but there are significant safeguards regarding use.	Organisations can undertake workplace monitoring with no or minimal safeguards.

Factors that are likely to safeguard the rights of data subjects	Factors that are likely to undermine the rights of data subjects
Whether there are limitations on how third parties, including public authorities, can use the data it accesses	
Public and private authorities may only use the data it accesses or receives from third parties for justified and limited purposes. For example, in the case of public authorities, for law enforcement, protection of public health and safeguarding national security.	Public and private authorities may freely use the data it access or receives from third parties. For example, public authorities which use this data to develop detailed and intrusive individual profiles to control their freedom of movement or access to economic opportunities (when not linked to legitimate aims such as law enforcement, protection of public health or safeguarding national security).
There are meaningful safeguards on data sharing between public authorities.	There are no or limited safeguards in relation to data sharing between public authorities.
Whether individuals have effective and enforceable rights and remedies in relation to the safeguards on third party access	
Clear and enforceable rights are in place to allow individuals to access their personal data.	Individuals have no rights or limited rights, to access their personal data
Individuals may readily seek judicial challenge of private and public authorities accessing their data, including surveillance measures.	Individuals have no or limited ability to seek judicial challenge of private or public authorities accessing their data, including surveillance measures.
Whether there is effective oversight	

Factors that are likely to safeguard the rights of data subjects	**Factors that are likely to undermine the rights of data subjects**
Police and intelligence services operate with clear judicial or other effective administrative oversight of their activities.	Police and intelligence services operate with no or limited judicial or other effective administrative oversight of their activities.
There is a data protection or similar regulator with active powers of oversight and enforcement.	There is no such regulator, or a regulator with limited powers and/or which is of limited effectiveness
It is common practice for transparency reporting by public authorities of surveillance measures. There are processes for public authorities' compliance to be audited.	No or limited transparency reporting of surveillance measures by public authorities, and no other mechanisms for proper accountability. No or limited processes for audit.
More general factors:	
The destination country has mature data protection and/or privacy laws in place.	There are some data protection and/or privacy laws in place, but there is little no evidence or effective implementation. Or, there are no data protection and/or privacy laws in place
There is a good record of respect for human rights (in particular the right to privacy, freedom of expression and access to justice).	There is a poor record of respect for human rights (in particular the rights to privacy, freedom of expression and access to justice).

Factors that are likely to safeguard the rights of data subjects	Factors that are likely to undermine the rights of data subjects
There is a legal framework governing the use of biometrics or facial recognition (such as general data protection laws or specific laws or regulations).	Significant use of biometrics or facial recognition by public authorities, with only limited or no laws, regulations or other safeguards relating to it.
There are partial UK adequacy regulations in relation to the country (which do not cover your restricted transfer). This will depend on the scope of the underlying assessment of the country and the reason why the adequacy regulations are only partial.	

Relevant provisions in the legislation

See UK GDPR Articles 9(1) and 4(14), and Recital 51 (external link)

Decision point

If you decide that the third-party access regime in the destination country provides appropriate legal protections. In this case, **you may proceed with the restricted transfer using the IDTA**.

Otherwise, you should move on to the next question.

Example

What is the likelihood of third-party access to the data (including surveillance)?

Considering the **specific circumstances of the transfer** that you identify in step one A, assess whether the circumstances of your proposed transfer are **likely to be of interest to third parties such as surveillance authorities**.

Here, you are not considering whether third party access (including surveillance) is occurring with or without safeguards, just the likelihood of it occurring at all.

You may have decided that some (but not all) types of third party access, including surveillance, do have appropriate protection in the destination country. In that case, you only need to consider the **likelihood** of those types of **concerning** third party access occurring.

What do I need to do?

Table E provides a guide on factors to look at to help you form a view as to how likely third party access or surveillance may occur in relation to your transfer. You should look at the factors in the round. You may wish to seek assistance with this from the importer.

Table E: Assessing the **likelihood** of third party access or surveillance

Factors to suggest that third party access or surveillance may not occur	**Factors to suggest that third party access or surveillance may occur**
Public authorities have not accessed similar data held by the importer, including by request, court order or other access.	Public authorities have accessed similar data held by the importer, including by request, court order or other access.
Organisations similar to the importer in the destination country, particularly within sectors, do not have evidence of receiving requests from public authorities or third parties to access data. (Trade or sector bodies may provide this information).	Organisations similar to the importer in the destination country have evidence of receiving requests from public authorities or third parties to access data.
The data is in the public domain.	The data is not in the public domain.
The data is more easily accessible by other means.	The data could be a key source of access to this information by public authorities or third parties.
There is no evidence that surveillance authorities in the destination country access large volumes of personal data.	There are reasonable grounds to believe that surveillance authorities in the destination country access large volumes of personal data.
Technical measures are in place which make surveillance less likely, eg encrypted or hashed data.	Technical measures are in place which make surveillance more likely such as mandated back door access and data in the clear.

The data is subject to protections for confidentiality or legal privilege.	The data is not subject to protections for confidentiality or legal privilege.

Decision point

If you decide that there is minimal risk of third-party access (including surveillance) to the data **you may proceed with the restricted transfer using the IDTA**

Otherwise you should move on to the next question.

Example

What is the risk of harm?

You should assess whether any **risk of harm** could be caused to data subjects if third party data access (including surveillance) occurs.

You may have decided that some (but not all) types of third party access, including surveillance, do have appropriate protection in the destination country. In that case, you only need to consider the **risk of harm** arising from those types of **concerning** third party access.

What do I need to do?

To help you in assessing the risk of harm to data subjects if **concerning** third party access occurs, you should look into the specific circumstances of the transfer, as you may have done for Table B in Step 2B.

This time, you should look at whether there are any particular risks to your transfer which may mean the data is likely to be of interest to public authorities or third parties in the destination country, and the harm to data subjects which may come from that interest.

Table F provides a guide to help you do this. The Table references different risk levels (low, moderate and high) and factors which may reduce or increase that risk, to help you form an overall view of the potential harm.

Table F: Assessing overall **risk of harm** to data subjects arising from the specific circumstances of the transfer caused by **third party access**

Level of risk of harm to data subjects	**Low**	**Moderate**	**High**
The columns set out examples of certain categories of data subjects and relevant types of data. This list is not exhaustive, nor determinative. We intend it to help indicate the likely risk of harm to data subjects associated with particular transfers. It is important that you assess risk of harm in each case by referring to the context of the transfer's specific circumstances and the likelihood of surveillance that the previous sections identify.	**Staff**		
	Basic employment contact details eg name, job title	Non-sensitive employment records eg CV, payroll history Passwords	Special category employment records, eg sickness or absence records, health information, equality monitoring data, criminal records Sensitive information, eg banking details
	Members of the public or consumers		
	Basic contact information, eg shipping details, marketing preferences	Buying preferences, order history, basic credit scores	Payment or banking details Passwords.

Level of risk of harm to data subjects	**Low**	**Moderate**	**High**
	Professionals, business contacts, suppliers		
	Basic contact information	Course of dealings, order history (non-sensitive)	Information relating to course of dealings or order history (sensitive) Payment or banking details Passwords (if shared externally)

Adjustments to the level of risk of harm to data subjects	**Factors which may reduce or increase the risk of harm to data subjects**	
The overall risk to data subjects increases or decreases, depending on how similar to the UK the regime of the destination country is for supporting the contractual rights and protections in the IDTA. For example, if the destination country regime is similar to the UK (albeit with some concerns), you may decide that categories of data which are in the	**REDUCE** **Similarity to level of UK protection**	**INCREASE** **Divergence from level of UK protection**

moderate risk box above, come low risk.		
The overall risk to data subjects increases if you know or reasonably believe that the data subjects and/or the categories of personal data would be of interest to third parties and/or public authorities.	**REDUCE**  **Lower level of interest to third parties and/or public authorities**	**INCREASE**  **Higher level of interest to third parties and/or public authorities**
The following may decrease the risk of harm to data subjects.	**REDUCE**  • The data subject has expressly confirmed that he has been informed of the potential risks of the transfer and has no concerns in relation to the same, and this has been documented. • There are **partial** UK adequacy regulations in relation to the country (which do not cover your restricted transfer).	

Decision point

If you decide that the risk of harm to data subjects is low, even if there is **concerning** third party access, **you may proceed with the restricted transfer using the IDTA**.

Otherwise you should move on to the next question.

Example

Are you able to put in place extra steps and protections to reduce the risk of harm to low?

You should consider whether you could apply any **extra steps and protections** to safeguard the data. If you could, you should consider what impact those measures would have on the risks you identify above.

Extra steps and protections can help safeguard the data by:

- reducing the risk of **concerning** third-party access occurring; and/or
- reducing the risk of harm to data subjects if **concerning** third-party access does occur.

There are a range of extra steps and protections that you can use, covering additional technical, organisational or contractual protections.

Of course these extra steps and protections are over and above the protections you established were already in place in Step 1.

Table G is a non-exhaustive list of measures that you may apply and guidance on how they may reduce potential harm to data subjects arising from **concerning** third party access. The table references different levels of risk reduction (basic, enhanced, significant) to help you form an overall view of the effectiveness of the measures.

You may need to change the IDTA to make sure the measures you use are a binding part of the IDTA.

Table G: Types and levels of measures to **supplement** IDTA safeguards

Type of additional measures	**Basic**	**Enhanced**	**Significant**
Access control *Reduces risk of **concerning** third party access taking place, and/or risk of harm if it does occur*	You will password protect data prior to transfer to importer. You will provide the password separately where the Importer is to process the data beyond storing it.	You will encrypt the data prior to transfer using an appropriate encryption solution (ie storage encryption / encryption at-rest) and you will implement suitable key management procedures	You will encrypt the data prior to transfer using appropriate encryption solution and you split the encrypted datasets between multiple parties.
Changes to data *Reduces risk of **concerning** third party access taking place, and/or risk of harm if it does occur*	You review the purposes and scope of the transfer and further minimise the amount of personal data you transfer (ie only certain data fields), but it is not anonymised or pseudonymised	You apply pseudonymisation techniques to the data prior to transfer and the importer does not have access to the additional information.	You split pseudonymised datasets between multiple entities, so that there is a minimal risk that any on party could identify a data subject. Note: You should also consider anonymisation techniques. If the data is effectively anonymised in the hands of a receiver so that it is no longer personal data, the UK GDPR transfer restrictions will not apply

Type of additional measures	Basic	Enhanced	Significant
Organisational *Reduces risk of **concerning** third party access outside of legal process in destination country and /or internal processes*	Both you and the importer offer regular staff training to raise awareness of data protection and security issues.	The importer does extra internal checks within its organisation to make sure data isn't being shared with third parties or public authorities, outside of the legal process in the destination country, and the organisation's internal processes. The importer strictly enforces password protocols	The importer strictly limits access to data to certain individuals with role-based access profiles. Where third parties or those without access privileges require access to data, they must follow a strict protocol before any data is shared more widely. Importer has a strict policy where it receives requests or legal orders for third-party access to data
Contractual *Reduces risk of **concerning** third party access outside of legal process in destination country*	The importer agrees to only allow access to data by third parties and public authorities unless strictly required by law, and to exhaust all rights of appeal.	The importer may comply with a request by a third party or public authority where the legitimate interests of the importer, the requesting party and any other third party override the interests or fundamental freedoms of the	If the importer receives a request from a third party or public authority for access to data it must: notify the exporter of the request, order or warrant and provide a copy of it; ask the law enforcement

Type of additional measures	Basic	Enhanced	Significant
		data subjects. The importer may comply with a request by a third party or public authority, where, if the request was made in the UK, the disclosure would be lawful and/or in the overriding public interest.	agency or public authority to redirect its request to the exporter to control conduct of the disclosure; if applicable, give the exporter the opportunity to withdraw or suspend the transfer; and challenge the validity of the request, order or warrant and demand that the public authority aims to obtain such information via co-operation with government bodies in each jurisdiction (ie use an alternative established treaty or mechanism to allow government-government sharing of obtain information). Importer must report monthly to the exporter if it receives no requests, orders or warrants relating to the exported data.

If the risk remains moderate or high, then you may need to do a more detailed risk assessment or consider relying on an exception. You may consider seeking professional advice before proceeding further.

If there is a high risk to any of the above, using an exception may be more appropriate and quicker, particularly for an urgent one-off transfer.

Recording your findings

You should document your overall findings from step three. Take account of your assessment of the surveillance regime, the likelihood of surveillance taking place, the risk of harm to data subjects and the impact of applying extra steps and protections. This should be sufficiently clear and detailed to provide a record of how you reach your assessment.

Example

Further reading – ICO guidance

We have produced guidance on security, encryption, controllers and processors and contracts.

Relevant provisions in the legislation

See UK GDPR Article 28 (3) and Recital 81

Decision point

If you decide:

- that risk of third-party access (including surveillance) to the data is minimal, you may proceed with the restricted transfer using the IDTA together with the extra steps and protections you identify
- the risk of harm to data subjects is low even if there is **concerning** third party access, you may proceed with the restricted transfer using the IDTA together with the extra steps and protections you identify.

Otherwise if you identify an enhanced risk of harm to data subjects which you cannot reduce by applying extra steps and protections, you cannot use our TRA tool for your risk assessment. In this situation, if you still wish to make the

restricted transfer, then you will need to carry out further steps in order to decide whether the transfer is lawful. You should do a more detailed risk assessment or consider relying on an exception. You may also consider seeking professional legal advice before proceeding further.

Guidance regarding extra steps and protections

Extra steps and protections may reduce the risks you identify with your transfer, which would otherwise prohibit it from taking place. Measures may be in the form of additional contractual, technical or organisational protections. You need to include those extra steps and protections as additional obligations in the IDTA, as security requirements or extra protection clauses.

You might want to contact the data importer for further advice as to the availability and effectiveness of any suggested extra steps and protections in the destination country. When they enter into the IDTA, they must promise that they have provided you with all relevant information regarding local laws and practices and the protections and risks which apply to the transferred data.

It may not be possible to reduce some risks (such as routine and unregulated access by national security or law enforcement agencies to personal data) using only contractual or organisational solutions. You may need to deploy sophisticated technical measures (such as advanced encryption techniques) to protect personal data even if someone accesses it. You may also need specialist technical security advice as to appropriate additional measures. In some cases, the cost of those extra steps and protections may outweigh the benefits of the proposed transfer.

You must ensure that any extra steps and protections do not contradict or undermine any of the appropriate safeguards the IDTA provides.

It is important to remember that there may not always be extra steps which reduce the risk. This may mean you cannot proceed with the transfer without changing your proposed transfer arrangements, for example by changing the type of data you want to transfer to be anonymised, pseudonymised or minimised, to reduce risk.

Have I covered everything I need to make a transfer decision?

You can go ahead with the restricted transfer if you:

- confirm that it meets the wider UK GDPR compliance requirements (as well as the international transfer rules);
- confirm that the transfer is not high risk or complex;

- assess and record the details of the restricted transfer;
- confirm that the contractual rights the IDTA sets out are likely to be enforceable and where there are concerns, the risk of harm to data subjects is low or can be reduced to low by additional steps and measures; and
- confirm that one of the following applies in the context of your restricted transfer:
    - the destination regime provides appropriate protections for third-party access to data (including surveillance);
    - the likelihood of third-party access (including surveillance) taking place is minimal (or becomes minimal once you apply any extra steps and protections); or
    - if **concerning** third-party access to data takes place, the risk of harm to data subjects is low (or becomes low once you apply any extra steps and protections).

Further reading

We have produced guidance on International Transfers

Relevant provisions in the legislation

See UK GDPR Article 45 and Recitals 103-107 and 169 and UK GDPR Article 49 and Recitals 111-112