

ICO TRA tool

Our [guidance on international transfers](#) details the requirement to carry out transfer impact assessments (TRAs). As set out in that guidance, there are different ways to carry out a TRA in order to meet legal requirements under the UK GDPR.

This ICO TRA tool is just one method that can be used to carry out a TRA but there are others, including the approach proposed by the EDPB. It is important that you keep a record of your assessment.

- You can use this template TRA tool to record your TRA. Importantly:
- You do not have to use this template. You can record your answers to the 6 questions in other ways.
- We have designed this template for a straightforward transfer, that is one where information is going only to one importer located in one destination country. You can adapt it for more complex personal information flows.
- Before using this TRA tool you should refer to our guidance to decide if and when a TRA is required in respect of your transfer.
- You may want to seek professional data protection advice to review your assessment.

The Appendix contains additional materials which may be helpful:

- A list of UK GDPR special category data.
- A list of typical categories of personal information with an initial risk score.
- Examples of extra steps and extra protections you may consider putting in place, which may be of assistance when carrying out this risk assessment.

Question 1: What are the specific circumstances of the restricted transfer?

Q1

Q2

Q3

Q4

Q5

Q6

Action required for Question 1:

Use Table 1 to document the specific circumstances of the transfer.

How do we complete this action?

- It is important that you record the **specific circumstances of the restricted transfer** including details of the importer, details of the people who the information is about, duration of the transfers, existing protections in place for the information and the categories of personal information being transferred.
- Use Table 1 to document this.
- If you are planning to use the IDTA as your transfer mechanism, you will need much of the same information. You can cross refer to other documents, such as the IDTA.

TABLE 1: Specific circumstances of the restricted transfer

Details of the importer

You may refer to other documentation here, such as the description included in the IDTA or other Article 46 transfer mechanism.

(1) Name of importer:

Who is the personal information going to?

(2) Destination country (or countries) of

<p>the personal information:</p>	
<p>(3) Status of the importer: See our guidance on controllers and processors for more information</p>	<p><input type="checkbox"/> controller <input type="checkbox"/> processor or sub processor <input type="checkbox"/> joint controller</p>
<p>(4) Importer's organisation: What kind of organisation is the importer?</p>	<p>The data importer's business or organisation is: Please tick all that apply</p> <p><input type="checkbox"/> Commercial <input type="checkbox"/> Public sector <input type="checkbox"/> Not for profit <input type="checkbox"/> Regulated in the destination country - add type of business (eg financial services, legal services, healthcare): <input type="checkbox"/> Other relevant features - add details:</p> <p><input type="checkbox"/> Part of a multi-national group - add name of group: <input type="checkbox"/> Large business (but not multi-national) - add details of size of group: <input type="checkbox"/> Small business or sole trader - add details of size of business:</p>
<p>(5) Importer's relevant activities What will the importer be doing with the information? Think about why the importer is using the personal information that will be transferred. You may be able to re-use a description of the importer's activities as set out in your service</p>	<p>The importer's activities or services that are relevant to the transfer are:</p>

contract with the importer.

For example:

“The importer is supplier of software solutions. It is supplying a software package to the exporter and will host the importer’s customer information on its servers in the US.”

Details of the people the information is about

You may refer to other documentation here, such as the description in the IDTA or other Article 46 transfer mechanism.

(6) Categories of people:

Who is the personal information about?

Think about who the personal information being transferred is about. Click in the box next to all of the categories of people who are included in the personal information being transferred. You may make appropriate amendments or add specific details to any of the categories or click “other” and add your own categories at the end.

The personal information transferred is about the following categories of people:

Confirm if the people are either or both:

- adults (who are not vulnerable) children or vulnerable adults

Tick all the categories that apply:

Each category includes current, past and prospective people the information is about.

If any of the following is a business or organisation, it includes their staff.

- | | |
|---|---|
| <input type="checkbox"/> staff including volunteers, agents, temporary and casual workers | <input type="checkbox"/> experts and witnesses |
| <input type="checkbox"/> customers and clients (including their staff) | <input type="checkbox"/> advisers, consultants and other professional experts |
| <input type="checkbox"/> suppliers (including their staff) | <input type="checkbox"/> patients |
| | <input type="checkbox"/> students and pupils |

	<input type="checkbox"/> members or supporters <input type="checkbox"/> shareholders <input type="checkbox"/> relatives, guardians and associates of the person the information is about <input type="checkbox"/> complainants, correspondents and enquirers	<input type="checkbox"/> offenders and suspected offenders <input type="checkbox"/> children and vulnerable adults <input type="checkbox"/> other (please provide details of other categories of people the information is about):
<p>(7) Volume</p> <p>How much personal information are you transferring?</p>	<p>For each person: the number of personal information categories (you can count these when you complete Table 2): (state if estimated or actual).</p> <p>For each transfer: the number of people the information is about (state if estimated or actual).</p> <p>Over the term of your contract or arrangement, the total number of people the information is about (state if estimated or actual).</p>	

<p>Duration</p> <p>You may refer to other documentation here, such as the description in the IDTA or other Article 46 transfer mechanism.</p>	
<p>(8) Frequency of transfers</p> <p>How often will these transfers occur?</p> <p>Think about how often information will be transferred to, or accessed in, the destination country. Delete and complete the wording as appropriate.</p>	<p>How often is a transfer made:</p> <ul style="list-style-type: none"> • once • every days/months/years • continuously for days/months/years
<p>(9) Duration of arrangement with</p>	<p>days/months/years</p>

importer

How long can the importer receive or access the information for?

You may cross-refer to a separate contractual provision here, or to a mechanism to determine the duration of the relationship (if your contract may be extended, or terminated early).

Protections for the transferred personal information

You may refer to other documentation here, such as the description included in the IDTA or other Article 46 transfer mechanism.

(10) Format of the personal information

What is the format of the transferred personal information?

For example, is it plain text or encrypted?

(11) Transfer process

How are you sending the personal information?

For example, are you transmitting it by email, website encryption or secure file transfer protocol (SFTP)? Or does the transfer involve remote access to personal information stored in the UK?

(12) Exporter's technical and organisational measures

By the exporter before transfer:

What other technological and organisational security measures will **you** put in place to protect the personal information before transfer?

Is the personal information pseudonymised?

13) Importer's technical and organisational measures

What other technological and organisational security measures will the **importer** have in place to protect the personal information once it has been received?

By the importer after receipt:

(14) Categories of personal information

What type(s) of personal information are you transferring?

Please complete the first column of Table 2 in Question 2 to record this information

Question 2: What is the level of risk to people in the personal information you are transferring?

Q1

Q2

Q3

Q4

Q5

Q6

Action required for Question 2:

Use Table 2 to assign a risk level to the personal information you are transferring.

How do I complete this action?

Using the information you recorded at Question 1, you must now **assign a risk level** to the personal information you are transferring.

We have set out below a description of what is a low, moderate and high harm risk, if the personal information is misused or lost.

- List in Table 2 below the categories of personal information you are transferring (you should have done this as part of Q1, Table 1 (14)). In the Appendix, there is a list of typical categories of personal information with an initial risk score (low, moderate or high harm risk). We recommend you use this as the starting point for assessing the risk level.
- UK GDPR specifies that certain types of personal information known as special category data need extra protection. There is a list of special category data in the Appendix. Special category data also includes types of information that can be used to infer any of the information on that list. For example, a photograph showing you attending a medical clinic which treats only a specific type of illness, is special category data because you can infer from that photograph that there is a high chance you have this illness.
- Consider if there are any factors that may increase or reduce that initial risk score. You can use Table 2 to keep a record of those factors. We have suggested some relevant factors, but there may be more.
- Give each category of personal information you are transferring a risk score (in the final column of Table 2). Take into account the initial risk score, any aggravating or mitigating factors identified, and the descriptions of the risk levels.

- At this stage you don't need to worry about the destination country.
- You may be able to reduce the risk score by making changes to the information you are transferring or adding in security protections before transferring it. If you wish to do so, make these changes and repeat Question 1 and 2.

Once you have completed Table 2, proceed to [Decision point A](#) to record your results.

Low harm risk	Unlikely to cause more than inconsequential financial harm, physical harm, mental harm or distress. Minimal actions required to put it right (if any), such as an apology.
Moderate harm risk	Unlikely to cause more than minor financial harm, physical harm, mental harm or distress. Some actions needed to put this right, such as proactively seeking the return of information or stopping its unauthorised spread. If this was a data breach, you may need to inform the ICO, but not the people the information is about.
High harm risk	Likely to cause significant financial harm, physical harm, mental harm or distress. Urgent action is required to put this right and minimise the harm caused. If this was a data breach, you would need to inform the ICO and the people the information is about.

TABLE 2: Personal information risk level

Note: This table is editable. Insert rows to add more categories if needed. You may add notes below the Y/N response to explain your decision.

Category of personal information List the categories.	Initial risk score (low, moderate or high)	Aggravating factors that tend to increase risk level	Mitigating factors that tend to reduce risk level	Other factors	Final risk score - Risk of harm to the people the information is
--	---	--	---	---------------	--

Decision point A (select relevant option):

Based on your assessment in Table 2, the level of risk to people in the categories of personal information you are transferring is:

1. **All** the categories of personal information we are transferring are a **low harm risk**.

Next step: You may proceed with the restricted transfer. This is because no matter what the response might be to the next questions, the nature of the personal information and the circumstances of the transfer means the risk of harm to people is low. You can record this as the final decision for your TRA.

2. **All** the categories of personal information we are transferring are **low harm risk** and **moderate harm risk**. (None is **high harm risk**)

Next step: go to Question 3.

3. **All or some** of the categories of personal information we are transferring are a **high harm risk**.

Next step: go to Question 3.

Additional notes:

Include any other information that may be relevant to your analysis and decision.

Question 3: What is a reasonable and proportionate level of investigation, given the risk level in the personal information and the nature of your organisation?

Q1

Q2

Q3

Q4

Q5

Q6

Action required for Question 3:

- Use Tables 3 and 4 to decide what is a reasonable and proportionate level of investigation of the destination country.
- Carry out and record the findings of your investigation.

How do I complete this action?

To decide the level of investigation required, you must consider three factors:

- Factor 1: the risk level in the personal information you identified at Question 2 (at [Decision point A](#)).
- Factor 2: the size of your organisation and therefore the resources available to you. Use the [data protection fee tiers](#) as a guide - organisations who are required to pay a Tier 1 or Tier 2 data protection fee are considered an SME for the purpose of this question.
- Factor 3: The total volume of personal information you are transferring. Transfers are high volume if you are sending a significant amount of personal information either in one transfer or in a number of recurring transfers.

Use the investigation matrix in Table 3 to decide the level of investigation required. The 3 levels of investigation are set out in Table 4. Make a note of which level of the investigation you are going to conduct and your reasons why this is reasonable and proportionate.

Carry out your investigation. First read Questions 4 and 5 below, because you will use the results of your investigation to answer those two questions.

If some or all of the personal information is high harm risk and you do not want to carry out a level 3 investigation, then at [Decision Point B](#) select “LEVEL 3 investigation Option (ii)”, and follow the instructions. It means you can carry out a level 2 investigation for your low and moderate risk data only, and that you can transfer the high harm risk data only if an exception applies (considered in Question 6).

TABLE 3: Investigation matrix

Business size	All the personal information we are transferring is low harm risk	All of the personal information we are transferring is low harm risk and a moderate harm risk	All or some of the personal information we are transferring is high harm risk
SME	No further investigation necessary. You may make your restricted transfer (see Decision point A).	<input type="checkbox"/> Level 1 investigation	<input type="checkbox"/> If you are transferring a low volume of personal information = Level 2 investigation <input type="checkbox"/> If you are transferring a high volume of personal information = Level 3 investigation
Large business		<input type="checkbox"/> Level 2 investigation	<input type="checkbox"/> Level 3 investigation

TABLE 4: Levels of investigation

Level 1 investigation	Level 2 investigation	Level 3 investigation
<p>Resources to use (Level 1): Consider:</p> <ul style="list-style-type: none"> • your own knowledge of the destination country, including its legal system, respect for the rule of law and its human rights record; • the latest Foreign Commonwealth and Development Office Human Rights and 	<p>Resources to use (Level 2):</p> <p>In addition to the resources in the previous column, you should carry out further internet-based research about the destination country, using reputable websites. This may include:</p> <ul style="list-style-type: none"> • additional human rights reports issued 	<p>Resources to use (Level 3):</p> <p>Option (i):</p> <p>In addition to using the resources in the previous two columns, you should conduct a detailed analysis about the treatment of human rights in the destination country.</p>

<p>Democracy Report;</p> <ul style="list-style-type: none"> the relevant Department for International Trade's Exporting country guides; and at least one human rights report, such as those published by charitable organisations (eg Amnesty International Reports on the state of the world's human rights). <p>You should always bear in mind what other influences may impact these reports, and therefore how much you can rely on them.</p>	<p>by charitable organisations;</p> <ul style="list-style-type: none"> human rights reports from other governments (eg US State Department's Country reports on human rights practices); and newspaper reports. <p>You should always bear in mind what other influences may impact these reports, and therefore how much you can rely on them.</p>	<p>You may need professional advice for this level of investigation.</p> <p>Option (ii): Mark all high harm risk data as "significant risk data", and carry out a Level 2 investigation for the rest of the information. You will not need to answer Question 5. Follow the instructions in Decision Point B.</p>
---	--	--

Decision point B: Make a note of the level of the investigation you are going to carry out, and your reasons why this is reasonable and proportionate.

LEVEL 1 investigation

LEVEL 2 investigation

LEVEL 3 investigation Option (i)

LEVEL 3 investigation Option (ii) Go to [Decision point E\(2\)](#) and tick that all your high harm risk data is both human rights risk data and enforceability risk data.

Carry out a level 2 investigation for your low and moderate risk data. Answer Question 4 and complete [Decision point C](#) for the low and moderate risk data only.

You do not need to answer Question 5. This is because low and moderate risk data cannot be enforceability risk data.

This means you can only transfer the high harm risk data if an exception applies (considered in Question 6).

Additional notes:

Include any other information that may be relevant to your choice of investigation.

Question 4: Is the transfer significantly increasing the risk for people of a human rights breach in the destination country?

Q1

Q2

Q3

Q4

Q5

Q6

Action required for Question 4:

- Based upon your investigation and the specific circumstances of the transfer, decide whether by making the transfer you are making the human rights risk worse for the people the information is about. This could be by making it more likely that a human rights breach will happen or by making it more severe if it did happen.
- The increase in risk must be clear and meaningful and linked to your transfer.
- Use Table 6 to record your investigation and to make your risk assessment.

How do I complete this action?

- You must consider the specific circumstances of the transfer and any other relevant factors which you can reasonably know, imply or predict. For example, do you know or is it likely that any of the people the information is about are citizens or residents of the destination country, is it reasonably possible they will travel to the destination country?
- Consider whether by making the transfer you are making the human rights risk worse for the people the information is about, by making it more likely that a human rights breach will happen or making it more severe if it did happen.
- Human rights are basic rights and freedoms for every person in the world. In the modern world they are founded on the Universal Declaration of Human Rights (adopted by the United Nations in 1948). This formed the basis of the European Convention of Human Rights (ECHR). Table 5 provides a summary of the key human rights taken from simplified ECHR.
- Use Table 6 to record the findings of your investigation and make your risk assessment

- If you have concerns that the transfer is significantly increasing the risk of a human rights breach for people, consider whether you can take any extra steps or put in place extra protections. The Appendix has examples and extra steps and protections for you to consider. If so, update your responses in in this TRA tool taking those extra steps and protections into account, and repeat this Question 4.

TABLE 5: Human rights risk analysis

<p>Art 1: Obligation to respect human rights</p>	<p>This is the general principle that countries must make sure everyone has these human rights.</p>	<p>Art 8: Right to respect for private and family life</p>	<p>You have the right to respect for your private and family life, your home and correspondence (letters, emails, phone calls, texts etc).</p>
<p>Art 2: Right to life</p>	<p>You have the right to life. Take note whether the death penalty is available for certain crimes.</p>	<p>Art 9: Freedom of thought, conscience and religion</p>	<p>You have the right to freedom of thought, conscience and religion.</p> <p>You have the right to practise your religion at home and in public and to change your religion if you want.</p>
<p>Art 3: Prohibition of torture</p>	<p>No one has the right to hurt you or torture you, even when you are held by police or armed forces.</p>	<p>Art 10: Freedom of expression</p>	<p>You have the right to responsibly say and write what you think and to give and receive information from others.</p> <p>This includes freedom of the press.</p>
<p>Art 4: Prohibition of slavery and forced labour</p>	<p>It is prohibited to treat you as a slave or to impose forced labour on you.</p>	<p>Art 11: Freedom of assembly and association</p>	<p>You have the right to take part in peaceful meetings and to set up or join associations -</p>

			including trade unions.
Art 5: Right to liberty and security	<p>You have the right to liberty.</p> <p>If you are arrested you have the right to know why.</p> <p>If you are arrested you have the right to stand trial soon, or to be released until the trial takes place.</p>	Art 12: Right to marry	You have the right to marry and to have a family.
Art 6: Right to a fair trial	<p>You have the right to a fair trial before an unbiased and independent judge.</p> <p>If you are accused of a crime, you are innocent until proved guilty.</p> <p>You have the right to be assisted by a lawyer who has to be paid by the state if you are poor.</p>	Art 13: Right to an effective remedy	If your rights are violated, you can complain about this officially to the courts or other public bodies.
Art 7: No punishment without law	You cannot be guilty of a crime if your action was not a crime at the time you did it.	Art 14: No discrimination	You have these rights regardless of your skin colour, sex, language, political or religious beliefs, or origins.

TABLE 6: Record of investigation and conclusions

Investigation level:	<input type="checkbox"/> 1 <input type="checkbox"/> 2
----------------------	--

	<input type="checkbox"/> 3
<p>Resources used:</p> <p>Make a note here of resources used (see Table 4)</p>	
<p>Key question 1: From your investigation do you have any concerns about any human rights issue?</p>	<p><input type="checkbox"/> No concerns. Go to Decision point C and tick C1.</p> <p><input type="checkbox"/> We have concerns, which are: refer to the specific Articles set out above, if you can. Go to Key question 2.</p>
<p>Key question 2: By making this transfer, are you making the risk significantly worse for the people the information is about?</p> <p>By either:</p> <ul style="list-style-type: none"> • making it more likely that a human rights breach will happen to the people the information is about; or • making the human rights breach more severe if it did happen. <p>The increase in risk must be clear and meaningful and linked to the transfer.</p>	<p><input type="checkbox"/> No. Go to Decision point C and tick C2.</p> <p><input type="checkbox"/> Yes.</p> <p>Which categories of personal information cause the increase in risk:</p> <p><input type="checkbox"/> All categories of personal information. Go to Decision point C and tick C3</p> <p><input type="checkbox"/> Only the following categories of personal information: (please list): Go to Decision point C and tick C4.</p>

Decision point C: Read and select the most appropriate response based upon your investigation:

1. **We do not have any concerns about any relevant human rights risk in the destination country for the people the information is about.**

Next steps: go to Q5.

2. **We have concerns that there are human rights risks in the destination country, but by making the transfer we are not significantly increasing the risk of a human rights breach in the destination country for the people the information is about.**

Next steps: go to Question 5.

3. **We have concerns that the transfer is significantly increasing the risk of a human rights breach in the destination country for the people the information is about, and this applies to all the categories of personal information.**

Next steps: Go to [Decision point E](#)(3) below and tick “**Yes, all categories of data are human rights risk data**”. If at Question 2 you selected a Level 3 Option (ii) investigation, move on to Question 6. Otherwise go to Question 5.

4. **We have concerns that the restricted transfer is significantly increasing the risk of a human rights breach in the destination country for the people the information is about, and this applies only to some categories of personal information.**

Next steps: Go to [Decision point E](#)(4) below, tick and list “**Yes, the following categories of data are human rights risk data**” and list them. If at Question 2 you selected a Level 3 Option (ii) investigation, move on to Question 6. Otherwise go to Question 5.

Question 5:

(a) Are you satisfied that both you and the people the information is about will be able to enforce the Article 46 transfer mechanism against the importer in the UK?

(b) If enforcement action outside the UK is needed: are you satisfied that you and the people the information is about will be able to enforce the Article 46 transfer mechanism in the destination country (or elsewhere)?

Q1

Q2

Q3

Q4

Q5

Q6

Action required for Question 5:

- Using the resources gathered as part of your investigation and taking into account the specific circumstances of the transfer, consider whether the transfer mechanism can be enforced against the importer in the UK or, if needed, in the destination country..
- Use Table 7 to record your risk assessment.

How do I complete this action?

- To answer question 5 we suggest that you work through the questions in the Table 7 Enforcement questionnaire
- If you have concerns about the enforceability of the transfer mechanism, consider whether you can take any extra steps or put in place extra protections. The Appendix has examples of extra steps and protections for you to consider. If so, update your responses in in this TRA tool taking those extra steps and protections into account, and repeat this Question 5.

TABLE 7: Enforcement questionnaire

Enforcement risk – Key questions	Answer	Notes															
<p>1. Are you transferring only personal information that gives rise to a low harm risk or a moderate harm risk (see Question 2)?</p>	<p><input type="checkbox"/> Yes. Go to Decision point D and tick D(1)</p> <p><input type="checkbox"/> No, go to next question</p>																
<p>2. In your investigation into the destination country, have you found any records suggesting there are issues about respect for the rule of law, independence of the Courts and Judges, and the time it takes for cases to be heard?</p>	<p><input type="checkbox"/> No concerns. Go to Decision point D and tick D(2).</p> <p><input type="checkbox"/> Yes (or not sure). Add notes and go to next question.</p>																
<p>3. Is there a high likelihood that the importer will accept the decision of a UK Court or arbitration award? Factors to consider here:</p> <p>(a) The importer has insurance from a reputable insurance provider that covers payment of claims in a UK Court or a UK arbitration award, without requiring any action to be brought in the destination country. The insurance must be enough to cover all of the potential claims. If this applies, you must check this insurance cover each year.</p> <p>(b) The importer has provided evidence that in the past it has always accepted decisions of UK Courts or UK arbitration awards.</p> <p>(c) The importer must comply with professional or similar rules, and you would be able to make a complaint to its oversight body, which would impact its ability to do business.</p>	<p>first tick if any of the factors apply</p> <table border="1" data-bbox="1064 774 1646 1141"> <thead> <tr> <th data-bbox="1064 774 1176 837">Factor</th> <th data-bbox="1176 774 1411 837">Satisfied</th> <th data-bbox="1411 774 1646 837">Not satisfied</th> </tr> </thead> <tbody> <tr> <td data-bbox="1064 837 1176 917">(a)</td> <td data-bbox="1176 837 1411 917"><input type="checkbox"/></td> <td data-bbox="1411 837 1646 917"><input type="checkbox"/></td> </tr> <tr> <td data-bbox="1064 917 1176 997">(b)</td> <td data-bbox="1176 917 1411 997"><input type="checkbox"/></td> <td data-bbox="1411 917 1646 997"><input type="checkbox"/></td> </tr> <tr> <td data-bbox="1064 997 1176 1077">(c)</td> <td data-bbox="1176 997 1411 1077"><input type="checkbox"/></td> <td data-bbox="1411 997 1646 1077"><input type="checkbox"/></td> </tr> <tr> <td data-bbox="1064 1077 1176 1141">(d)</td> <td data-bbox="1176 1077 1411 1141"><input type="checkbox"/></td> <td data-bbox="1411 1077 1646 1141"><input type="checkbox"/></td> </tr> </tbody> </table> <p>Taking these factors into account answer Question 3. If you are satisfied about one or more of the above factors, it is likely you may answer Yes.</p> <p><input type="checkbox"/> Yes. There a high likelihood that the</p>	Factor	Satisfied	Not satisfied	(a)	<input type="checkbox"/>	<input type="checkbox"/>	(b)	<input type="checkbox"/>	<input type="checkbox"/>	(c)	<input type="checkbox"/>	<input type="checkbox"/>	(d)	<input type="checkbox"/>	<input type="checkbox"/>	
Factor	Satisfied	Not satisfied															
(a)	<input type="checkbox"/>	<input type="checkbox"/>															
(b)	<input type="checkbox"/>	<input type="checkbox"/>															
(c)	<input type="checkbox"/>	<input type="checkbox"/>															
(d)	<input type="checkbox"/>	<input type="checkbox"/>															

Enforcement risk – Key questions	Answer	Notes
<p>(d) There are strong commercial reasons for the importer to accept a decision of UK Court or UK arbitration award, even where the claim is substantial.</p>	<p>importer will accept the decision of a UK Court or UK arbitration award. Add notes and go to Decision point D and tick D(3).</p> <p><input type="checkbox"/> No. There is not a high likelihood that the importer will accept the decision of a UK Court or arbitration award. Add notes and go to next question.</p>	
<p>4. Are there any other factors that make it very unlikely you or the people the information is about would have to bring a claim in the destination country to enforce the Article 46 transfer mechanism?</p>	<p><input type="checkbox"/> Yes. Set out the factors in the Notes, and go to Decision point D and tick D(4).</p> <p><input type="checkbox"/> No. Go to Decision point D and tick D(5).</p>	

Decision point D: Read and select the most appropriate response based on your investigation

1. We are only sending information that poses a low harm risk or a moderate harm risk.

As a result, there is a low likelihood that we and the people the information is about would need to enforce the transfer mechanism in the destination country.

2. We do not have any concerns about respect for the rule of law, independence of the Courts and Judges, and the time it takes for cases to be heard in the destination country.

3. There is a high likelihood that the importer would accept the decision of a UK Court or UK arbitration award (considering the factors set out in Table 7 above).

4. It is very unlikely that we or the people the information is about would have to bring a claim in the destination country to enforce the Article 46 transfer mechanism (considering the factors set out in Table 7 above).

5. We have concerns that (a) both we and the people the information is about may not be able to enforce the Article 46 transfer mechanism against the importer in the UK; and (b) if enforcement action is needed outside of the UK, we and the people the information is about may not be able to enforce the transfer mechanism in the destination country.

Go to [Decision point E\(5\)](#) and tick that “**All high risk data is enforceability risk data**”

Decision point E: Have you identified any **human rights risk data** at Question 4 or **enforceability risk data** Question 5?

If you are carrying out a Level 3 Option (ii) investigation, then you **must** tick E(2) and you **may** need to tick either 2 or 3 depending on your answers to Question 4.

1. **No**, we have not identified any because we have ticked:

- A(1);
- Or:
 - one of C(1) or C(2); **and**
 - one of D(1) or D(2) or D(3) or D(4).

You may proceed with the transfer.

2. **Yes**, all **high risk data** is both human rights risk data and enforceability risk data, because we ticked B(3) Option (ii).

(Optional) list all the categories of high risk data:

3. **Yes**, all **categories of data are human rights risk data**, because we ticked C(3).

(Optional) List all categories of data:

4. Yes, the following categories of data are human rights risk data, because we ticked C(4):

List the categories of data which, by including in the restricted transfer, you have concerns will significantly increase the risk of a human rights breach in the destination country for the people the information is about:

5. All high risk data is enforceability risk data, because we ticked D(5)

(Optional) list all the categories of high risk data:

The human rights risk data and enforceability risk data identified above is your “significant risk data” for Question 6

Question 6: Do any of the exceptions to the restricted transfer rules apply to the significant risk data you have identified?

Q1

Q2

Q3

Q4

Q5

Q6

Action required for Question 6:

- Your significant risk data is identified in [Decision point E](#).
- Using our [guidance](#) on the exceptions to the international transfer rules, and taking into account the specific circumstances of the transfer, and the type of risk you identified at [Decision point E](#), decide if any of the exceptions apply to the significant risk data.
- You are considering if one of the exceptions applies only for the significant risk data, and on the basis that the Article 46 transfer mechanism provides some (but not all) of the appropriate safeguards and effective and enforceable people's rights.
- You can only rely on these exceptions in very limited circumstances, if it is necessary and proportionate to do so.
- Use Table 8 to record your assessment.

How do I complete this action?

This question assumes you are putting in place the Article 46 transfer mechanism and all the extra step and protections you identified in working through this TRA tool.

To answer question 6 we suggest that you work through the questions in the Table 8 Exceptions checklist.

When thinking about whether the risks are outweighed by the benefits of the transfer, it may help to think about whether it is a human rights risk or an enforceability risk or both (as you identified in [Decision point E](#)).

If the exceptions do not apply to **all** the significant risk data, consider if you can take out of your restricted transfer the significant risk data that is not covered by an exception. If so, repeat the TRA tool removing that data.

TABLE 8: Exceptions checklist

Exception	Does the scenario apply?	Which types of significant risk data does the scenario apply to? (You can state all if the exception scenario could apply to all the significant risk data.)	Does the benefit of the transfer for this exception, outweigh all the risk(s) you identified in Decision point E	Your reasons
<ul style="list-style-type: none"> The person has given their explicit consent to the restricted transfer of the significant risk data. 	<input type="checkbox"/>		Not required for this exception	
<ul style="list-style-type: none"> The transfer of the significant risk data is necessary for the performance of a contract between you and the person the information is about. Or it is necessary so you can implement pre-contractual measures requested by that person. 	<input type="checkbox"/>		<input type="checkbox"/> Yes <input type="checkbox"/> No	
<ul style="list-style-type: none"> The transfer of the significant risk data is necessary for you to either perform or enter into a contract with a person, and that contract is in the interests of a separate person 	<input type="checkbox"/>		<input type="checkbox"/> Yes <input type="checkbox"/> No	

(who the information is about)				
<ul style="list-style-type: none"> The transfer of the significant risk data is necessary for important reasons of public interest. 	<input type="checkbox"/>		<input type="checkbox"/> Yes <input type="checkbox"/> No	
<ul style="list-style-type: none"> The transfer of the significant risk data is necessary for you or another person or organisation, to establish whether you or a third party has a legal claim or defence, to make a legal claim or to defend a legal claim. 	<input type="checkbox"/>		<input type="checkbox"/> Yes <input type="checkbox"/> No	
<ul style="list-style-type: none"> The transfer of the significant risk data is necessary to protect the vital interests of a person – this may or may not be the person the information is about. To use this exception the person the information is about must be physically or legally incapable of giving consent to the transfer of their information. 	<input type="checkbox"/>		<input type="checkbox"/> Yes <input type="checkbox"/> No	
<ul style="list-style-type: none"> The transfer of the significant risk data is from a public register and meets the relevant legal 	<input type="checkbox"/>		<input type="checkbox"/> Yes <input type="checkbox"/> No	

requirements about access to that public register.				
<ul style="list-style-type: none"> The restricted transfer of the significant risk data is necessary for your compelling legitimate interests. You must read our guidance about the extra requirements for this exception. 	<input type="checkbox"/>		<input type="checkbox"/> Yes <input type="checkbox"/> No	

Decision point F: Read and select the most appropriate response based on your analysis:

1. One or more of the exceptions applies to all the significant risk data. You may proceed with the transfer.

2. The exceptions do not apply to all the significant risk data. You may **not** proceed with the transfer relying on the Article 46 transfer mechanism.

If you are concerned whether you have reached the right conclusion, you may always seek professional data protection advice to review your assessment.

Additional notes:

include any other information that may be relevant to your analysis, including if you have decided to rely on an exception for certain categories of information, and remove other categories from the scope of the transfer.

Appendix to TRA tool

This Appendix sets out information which may be helpful to you when filling out your TRA Tool. It does not form part of your TRA Tool. You may delete this Appendix from your TRA Tool.

1. List of Special Category Data

Personal information revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership

Processing of genetic data or biometric data for the purpose of uniquely identifying a natural person

Personal information concerning:

- A person's health
- A person's sex life or sexual orientation

[Read our guidance on special category data.](#)

2. Categories of Personal Information

Please find below the relevant initial risk scores to apply when listing the different categories of personal information in Table 2 of the TRA tool.

Category of Personal Information	Initial risk score (indicative ICO score)
----------------------------------	--

Name	Low
Address & Contact details	Low
Age / DOB	Low
Gender	High
Biometric data	High
CCTV, photos and other images (which are not biometric data)	Moderate
Race/ethnic origin	High
ID documentation, such as passport, national insurance number, ID card, driving licence details	High
Medical records	High
Medication records	High

Name and contact details of GP	Low
Name and contact details of specialist medical professionals	High
Genetic data	High
Current marriage and partnerships	Moderate
Marital history	Moderate
Details of family and other household members	Moderate
Habits	Low
Housing	Low
Travel details	Low
Leisure activities	Low
Location Data	High

Membership of charitable or voluntary organisations	Low
Political opinions	High
Religious or philosophical beliefs	High
Trade Union membership	High
Sex life or sexual orientation	High
Free text about an individual, eg in emails, social media, livechat (must assume is SCD)	High (may vary depending on circumstances)
Employment and career history	Low
Recruitment	Low
Termination details	High
Attendance records	Low

Health and safety records	High
Performance appraisals	Moderate
Training records	Low
Security records	Low
Financial account / credit card details	High
Income	Moderate
Salary	Moderate
Assets and investments	Moderate
Payments	Moderate
Creditworthiness / Credit score	Moderate
Loans	Moderate

Benefits	Moderate
Grants	Moderate
Insurance details	Moderate
Pension details	Moderate
Goods or services supplied	Low
Marketing preferences	Low
Delivery preferences	Low
Licences issues	Low
Insurance details	Low
Records of unspent criminal convictions and offences	High
Records of spent criminal convictions and offences	High

Records of DBS checks	High
Criminal investigations records	High

3. Extra Steps and Protections

Questions 4 and 5 of the TRA tool ask you to consider whether you can take any extra steps and extra protections that will reduce the risks in relation to the restricted transfer.

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 which you already have in place, which you will have included in Question 1.

The table below is a **non-exhaustive example list** of measures that you may apply to seek to reduce the risks to the people the information is about, established by your investigation into the destination country. The table references different levels of risk reduction (basic, enhanced, significant) to help you form an overall view of the likely effectiveness of the measures.

To make sure the measures you use are legally binding, you may need to amend the Article 46 transfer mechanism. The effectiveness of these measures in reducing the risk to the person who the information is about will vary depending on the circumstances of the restricted transfer.

Extra Steps and Protections (examples only)

Category	Purpose	Basic Protection	Enhanced Protection	Significant Protection
----------	---------	------------------	---------------------	------------------------

Category	Purpose	Basic Protection	Enhanced Protection	Significant Protection
Access controls	Either minimises likelihood of a breach of the Art 46 transfer mechanism occurring or reduces risk of harm to the person who the information is about if a breach of the Art 46 transfer mechanism occurs	<p>You will password protect personal information prior to transfer to importer.</p> <p>You will provide the password separately where the importer is to process the personal information beyond storing it.</p>	You will encrypt the personal information 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 personal information prior to transfer using appropriate encryption solution, you will split the encrypted datasets between multiple parties and you will take measures to ensure the decryption code is retained only by you.
Changes to the personal information	Either minimises likelihood of a breach of the Art 46 transfer mechanism occurring or reduces risk of harm to the person who the information is about if a breach of Art 46 transfer mechanism occurs	You review the purposes and scope of the transfer and further minimise the amount of personal information you transfer (ie only certain data categories), but it is not anonymised or pseudonymised	You minimise the amount of personal information you transfer, apply pseudonymisation techniques to the personal information prior to transfer and the importer does not have access to the additional information.	<p>You only transfer minimal pseudonymised datasets and split them between multiple entities, so that there is a minimal risk that any one party could identify a person.</p> <p><u>Note:</u> You should also consider anonymisation techniques. If the personal information is effectively anonymised in the hands of a receiver so that it is no longer personal information, the UK GDPR transfer</p>

Category	Purpose	Basic Protection	Enhanced Protection	Significant Protection
				restrictions (and the UK GDPR generally) will not apply to that anonymised information.
Organisational	Reduces risk concerning (i) third party access to personal information outside of legal process in the destination country; and (ii) human rights breach for the person who the information is about in the destination country	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 personal information is not 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.	<p>The importer strictly limits access to personal information to certain individuals with role-based access profiles. Where third parties or those without access privileges require access to personal information, they must follow a strict protocol before any personal information is shared more widely.</p> <p>Importer has a strict policy where it receives requests or legal orders for third-party access to personal information.</p>

Category	Purpose	Basic Protection	Enhanced Protection	Significant Protection
Contractual	Additional contractual clauses in transfer mechanism to reduce risk of (i) exporter or the person who the information is about from being unable to enforce contractual rights; and (ii) third party access to personal information outside of legal process in destination country	Importer and/or exporter has an enhanced complaints process for people whose personal information has been subject to a data breach, including a compensation scheme.	<p>If exporter has sufficient financial resources: contractual right for people to bring a claim against the exporter if the importer fails to comply with UK court order or arbitration award.</p> <p>The importer may only comply with a request by a third party or public authority (i) where the legitimate interests of the importer, the requesting party and any other third party override the interests or fundamental freedoms of the person who the information is about ; or (ii) if the request was made in the UK, the disclosure would be lawful and/or in the overriding public interest.</p>	<p>If exporter has sufficient financial resources: contractual right for people to bring a claim against the exporter for any breach of the Article 46 transfer mechanism by importer.</p> <p>Or a contractual right for people to bring a claim against a UK organisation in the same group as the importer (with sufficient financial resources) for breach by the importer.</p> <p>Confirmation and commitment by importer to maintain:</p> <ul style="list-style-type: none"> • Professional or regulatory status • ICO code of conduct • ICO certification • Reputable security certification <p>If the importer receives a request from a third party</p>

Category	Purpose	Basic Protection	Enhanced Protection	Significant Protection
				<p>or public authority for access to personal information it must:</p> <ul style="list-style-type: none"> • notify the exporter of the request, order or warrant and provide a copy of it; • ask the law enforcement 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

Category	Purpose	Basic Protection	Enhanced Protection	Significant Protection
				<p>established treaty or mechanism to allow government-government sharing of obtain information).</p> <ul style="list-style-type: none">• Importer must report monthly to the exporter if it receives no requests, orders or warrants relating to the exported personal information.