STEPHENSON HARWOOD

See EU later

Using the UK's post-Brexit data transfer tools

On 11 August 2021, the Information Commissioner's Office ("ICO") published a consultation on proposals to update its guidance on international transfers of personal data ("Guidance"), a new transfer risk assessment ("TRA") and an international data transfer agreement ("IDTA"). A draft addendum to the European Commission's standard contractual clauses ("SCCs") was also published ("UK Addendum"), which will enable the EU SCCs to be used in a UK context, as an alternative to the IDTA. The Guidance, TRA and IDTA are notably different to their EU counterparts, which will provide a challenge to organisations operating both within the EU and the UK.

These tools and the new Guidance are expected to be finalised by the end of 2021. It is proposed that all existing UK transfers documentation must be replaced with the new approved versions within three months for new transfers and within a total of 24 months for all existing transfers. The new documents will therefore be critical to those organisations transferring or receiving personal data that is subject to the UK General Data Protection Regulation ("GDPR")".

The consultation comes during a period of significant change for international data transfer regimes:

- The decision of the Court of Justice of the European Union in the "*Schrems II*" case in July 2020 placed a new focus on assessing the laws of the recipient jurisdiction, to ensure that personal data transferred outside of the UK or EU is given essentially equivalent protection to that available domestically. The European Data Protection Board set the tone for assessing the risk in international transfers in their recommendations on supplementary measures for international transfers ("**EDPB Recommendations**").
- Following Brexit, the EU's ("**GDPR**") became part of the domestic laws of the UK ("**UK GDPR**") and the UK was granted adequacy decisions by the European Commission. For the time being, therefore, no additional safeguards are needed in relation to data flows between the UK and EU.
- Most recently, we saw the European Commission publish new **SCCs** to safeguard international transfers of data from the EU, a significant update on the previous versions.

This guide will break down the ICO's new transfer tools in the context of these three developments, by explaining what the TRA and IDTA do, how they address the requirements arising out of *Schrems II* and how they differ from their European equivalents, namely the SCCs and EDPB Recommendations.

Consultation

The ICO has launched a consultation seeking views on the Guidance, the draft IDTA and TRA, and the UK Addendum.

In relation to the Guidance, the ICO has opened up fundamental questions relating to the extra-territorial effect of the UK GDPR and restricted transfers. Two of the key questions that the consultation asks are:

- Whether processing by an overseas processor whose controller is subject to the GDPR should be considered in scope of UK GDPR on the basis that its processing is carried out in the context of the activities of a UK-based controller, or if its processing relates to the controller's overseas activity.
- Whether a transfer from a processor which is subject to the UK GDPR to its controller which is not subject to the UK GDPR should be considered a restricted transfer.

This will have an impact not just on international transfers, but on wider assessments of whether certain organisations are subject to the UK GDPR at all.

The consultation closes at 5pm on 7 October 2021 and you can have your say **here**.

We can help organisations implement these new transfer tools strategically and pragmatically. Please contact us to find out how we can help you navigate the IDTA, TRA and the ICO's updated approach to international transfers.

Contact us

Katie Hewson

Partner, data protection

T: +44 20 7809 2374
E: katie.hewson@shlegal.com

Olivia Fraser

Associate, data protection

T: +44 20 7809 2844
E: olivia.fraser@shlegal.com

The International Data Transfer Agreement

What is the IDTA?

What is the IDTA? The IDTA is an appropriate safeguard to be used where there is a restricted transfer of personal data under the UK GDPR. It will function as an approved, standard form safeguard under the UK GDPR, and is the UK's equivalent to the SCCs.

What is the structure of the IDTA? The IDTA is made up of four different parts:

- Part 1: This section is for specific transfer details and includes four tables to be completed.
- Part 2: This provides for extra protection clauses to be added, which are optional but should be added where a TRA has indicated they are required.
- Part 3: This part allows the parties to insert additional commercial clauses if desired.
- Part 4: This section includes mandatory clauses which cannot be changed and must be included in every IDTA ("**Mandatory Clauses**").

How to use the IDTA

How do you enter into the IDTA? The IDTA is intended to be a legally binding agreement between the parties, so the easiest and simplest way to enter into the IDTA is by signing it. However, the ICO has specified that the parties can choose other methods to enter into the IDTA, providing that the full IDTA binds the parties.

How does it work alongside my other agreements? The ICO has recognised that the IDTA is likely to be linked to other agreements between the parties such as service agreements or data sharing or processing agreements ("**Linked Agreements**"). To ensure that data subjects' rights are not compromised as a result of discrepancies between the Linked Agreements and the IDTA, the IDTA will prevail, unless the conflicting provisions provide greater protection to data subjects or are expressly required by Article 28 of the UK GDPR.

What are your obligations under the IDTA?

The Part 4 Mandatory Clauses set out the obligations of the exporter and the importer in relation to restricted transfers. In particular:

Rights of the ICO: Importers and exporters agree to provide the ICO with certain information, including the IDTA, any TRAs, and the importer's information regarding local laws. As a result, importers will have direct obligations to the ICO, even where they have no other connection to the UK.

Data subject requests: Where a data subject requests a copy of the IDTA from the exporter or importer, this must be provided. Where the commercial clauses in Part 3 of the IDTA are used, the parties may redact that section, but a summary of the information must be provided. Where a Linked Agreement is used, the parties do not need to disclose that Linked Agreement.

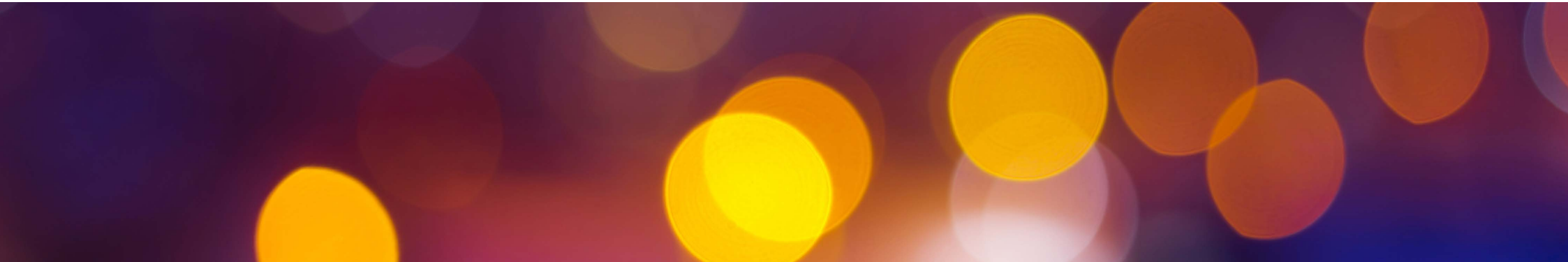
Liability: There is uncapped liability for a breach of the IDTA causing damage to a data subject, and this cannot be derogated from in the commercial clauses or any Linked Agreements.

Significant Harmful Impact (SHI): This is a new concept introduced in the IDTA which provides for various termination rights where there is more than a minimal risk of a breach of the IDTA that may cause significant damage to a data subject or a party. Where there is a breach that causes a SHI, the importer must take steps without undue delay to end the SHI. The exporter must suspend transfers under the IDTA while the SHI is ongoing.

Importer obligations: Under the IDTA, the importer must:

- Keep a written record of its processing, which demonstrates its compliance with the IDTA.
- Provide a copy of the written record to the exporter upon request.
- Afford the same rights of audit to the exporter as set out in any Linked Agreement.
- Only make an onward transfer where it is entitled to do so, where the third party has entered into a contract with the importer offering the same level of protection to data subjects as the IDTA, the third party is a party to the IDTA, the transfer would comply with the UK GDPR, or the transfer is to an adequate country.
- Where there is a breach by the importer that is likely to result in a risk to the rights or freedoms of any data subject, notify the exporter without undue delay (with more obligations owing if this risk is a high one).

Local laws: The importer must have provided the exporter with all relevant information regarding local laws and practices and the protections and risks that apply to the data before entering into the IDTA. This information must be complete, accurate and adequate to allow the exporter to complete a TRA. The importer must represent that they are not aware of any local laws that contradict their IDTA obligations and agree to co-operate to ensure compliance. Critically, both parties represent that the security requirements and extra protection clauses provide a level of security which is appropriate to the risk of a breach and the impact on data subjects.



Application of the IDTA

When does the IDTA apply?

Who should use the IDTA? As with the SCCs, the IDTA should be used where there is a "restricted transfer" taking place between an exporter and an importer. If you are subject to the UK GDPR and you are transferring, or making data available to a recipient in a separate organisation in a third country, you should consider whether (a) there is a restricted transfer and (b) the IDTA applies to the data flow.

What is a restricted transfer: to what data flows does the IDTA apply?
This is one of the key unanswered questions to be settled in the ICO consultation. The IDTA may apply to transfers between exporters and importers where:

- The exporter in question is subject to the UK GDPR.
- The importer is either (i) not subject to the UK GDPR (and so the data is leaving the protection of UK GDPR); **OR** (ii) located outside of the UK (whether (i) or (ii) is correct will be considered in the consultation).
- The importer is a separate company or individual to the exporter.

The IDTA will apply to the following types of transfer:

An exporter which is subject to the UK GDPR or is located in the UK	Transfers to	An importer which is not subject to the UK GDPR or is located outside the UK
Any controller/joint controller	➡	Another controller OR its processor
Any processor	➡	Its sub-processor
Any processor with a controller subject to UK GDPR	➡	Any third party that is not its controller or sub-processor
Any sub-processor	➡	Its sub-sub-processor
Any sub-processor with a controller subject to UK GDPR	➡	Any party that is not its controller or processor

One notable type of transfer to which the IDTA will not apply is transfers from processors whose processing is subject to the UK GDPR, where the controller is not subject to the UK GDPR. This is because this **is not** considered a restricted transfer.

Do I need the IDTA as well as the SCCs?

In recognition of the fact that many organisations are likely to be subject to both the UK and the EU GDPR, and in an attempt to reduce the risk of multiple sets of documents for restricted transfers, the ICO has developed the UK Addendum. This would work alongside the European Commission's SCCs to apply them in a UK context, as an alternative to the IDTA. An addendum model is also being considered for use with model data transfer agreements approved by other jurisdictions, such as the model clauses used by New Zealand and Association of Southeast Asian Nations.

The UK Addendum will offer organisations operating in the UK and EU a simpler and more streamlined transfer tool for safeguarding restricted transfers. Choosing whether to use the IDTA, the SCCs, or both, will require organisations to understand the differences, which are summarised below. There are also key practical challenges in deciding how and when to update UK and EU transfer documentation, given that the IDTA and UK Addendum are not expected to be finalised before the end of 2021, whereas the SCCs are already being rolled out.

IDTA vs SCCs: the difference between the UK and EU

The IDTA is notably different from the SCCs in format and usability. The key differences are set out below. These will have significant implications for organisations faced with implementing the IDTA in conjunction with the roll-out of updated SCCs.

Overall, the IDTA provides a more adaptable model than the SCCs: it is relatively simple to understand, populate and review. However, where organisations are already in the process of updating their EU SCCs, it seems increasingly likely that the UK Addendum option will be favoured by many in the short term, where necessary to avoid applying two separate sets of model clauses to a transfer under GDPR and UK GDPR. Regardless, some additional repapering is going to be required once the IDTA is approved by Parliament.

Format

Use of tables: The IDTA uses a table structure that enables users to complete it as if they were filling out a form. Although the use of this tabular format is optional, it does offer a simple option for setting out all the specific details of the transfer, including details of the parties, the categories of personal data being transferred, and the purposes of the transfer.

Plain English: The language of the IDTA is much simpler than the SCCs, with legal jargon being rejected in favour of plain English. This makes the IDTA more accessible to those without data protection expertise. The IDTA also requires an importer acting as a controller to be able to easily communicate with data subjects in English without undue delay.

Single Agreement: The IDTA does not use the modular format adopted by the EU Commission for the SCCs but is one single agreement. As a result, certain clauses in the IDTA are automatically disapplied in particular scenarios.

For example, clause 21 of the Mandatory Clauses sets out how individuals can exercise their data subject rights, but it only applies if the importer is the exporter's processor or sub-processor. While irrelevant clauses in the IDTA may be deleted if desired, businesses may find it simpler not to have to spend time extracting or integrating different modules.

Flexibility: Parties are free to edit the tabular element of the IDTA and delete irrelevant sections. The IDTA also expressly reflects that parties may have Linked Agreements (either in the form of a master service agreement or data processing agreement) to which parties might want to refer.

Controlling party: Parties can make the IDTA a multi-party agreement, if necessary to take account of data flows, and can even appoint one party to make decisions on everyone's behalf. This provides a commercial solution that is not inherently available under the SCCs.

Application

Data flows: The IDTA covers more scenarios than the EU SCCs, with processors being able to use the IDTA to transfer data to a third-party recipient that is not its controller or sub-processor (as long as the controller is subject to the UK GDPR). They can also be used for transfers between joint controllers.

Processor to controller: As mentioned above, the IDTA does not apply to cross-border transfers from processors that are subject to the UK GDPR to controllers that are not subject to the UK GDPR. This is a marked difference from the SCCs, which include a module for any processor to controller transfers.

Restricted transfers: Recital 7 of the European Commission's implementing decision accompanying the SCCs provides: "the [SCCs] may be used for such transfers only to the extent that the processing of the importer does not fall within the scope of [GDPR]". It follows that where the importer is directly regulated by GDPR then the SCCs should not be used to safeguard the transfer.

In the draft IDTA, the ICO's proposal for a restricted transfer to which the SCCs could apply is a transfer where:

- the UK GDPR applies to the data being transferred
- the data is being sent or made accessible to a receiver to which the UK GDPR does not apply **OR** who is located in a country outside the UK.

Depending on the outcome of the consultation, the IDTA could potentially be used even where the importer is subject to the UK GDPR, as a result of its extra-territorial effect under Article 3(2). This would be different to how the SCCs apply.

This question is one of the key considerations in the ICO's consultation on its Guidance.

The outcome of the consultation on this point will be much anticipated as it could result in the IDTA only being required for transfers to recipients **not** directly subject to the UK GDPR by virtue of its extra-territorial scope.

Content

The content of the IDTA is broadly similar to that of the SCCs, albeit drafted and structured differently.

Transparency: Both the IDTA and the SCCs require importers to provide certain information to data subjects, normally through a privacy notice. Although the IDTA does not explicitly state that this can be provided through the exporter (in contrast to the SCCs), there is no obligation to provide a notice directly to data subjects. Parties may wish to consider allocating responsibility for this in commercial clauses or Linked Agreements.

Conflict provisions: The IDTA prevails over conflicting provisions in a Linked Agreement unless the conflicting provision in the Linked Agreement provides greater protection or is expressly required by Article 28. The SCCs on the other hand do not have these exceptions. The IDTA, therefore, allows the parties greater control over their Article 28 contracts, which will benefit processors.

Arbitration: The ICO has suggested that a specific IDTA arbitration scheme could be introduced as a potential dispute resolution mechanism, for claims involving the ICO or data subjects. This type of specific arbitration scheme would be new in the context of data transfers.

Aligning the IDTA and the SCCs

As explained above, the European Commission published new SCCs in June which are due to replace the older versions from 2001, 2004 and 2010 ("**old SCCs**") by 27 September 2021. From that day, parties must stop using the old SCCs for new transborder flows and switch to the new SCCs, with existing contracts to be updated by 27 December 2022.

Following Brexit, UK data protection law only provides for the use of safeguards that were in force as at 31 December 2020, meaning UK law does not recognise the new SCCs. The IDTA will not be available in its final form until after the new SCCs are in force. This will leave a period during which organisations must use the new SCCs for EU GDPR but the old SCCs for UK GDPR. For those businesses that have already implemented the new SCCs for the EU transfers, they are also going to have to revisit their international transfer documents if the IDTA is approved.

The Transfer Risk Assessment

The TRA tool: when is it needed?

Restricted transfers: The Guidance is clear that a TRA must be completed where there is a restricted transfer and the parties seek to rely on an Article 46 UK GDPR transfer mechanism, such as the IDTA. A TRA will not be required if you are making a restricted transfer to any country deemed adequate by the UK government or if the restricted transfer is covered by one of the derogations under Article 49 of the UK GDPR.

Voluntary: The risk assessment itself is mandatory following *Schrems II* but the ICO's TRA model is not mandatory: organisations are free to use other methods of risk assessment that are already in place. The tool does however offer a good, practical option for such exercises, as it is indicates what the ICO considers to be important when carrying out mandatory risk assessments.

Routine transfers: The ICO only intends the TRA tool to be used to assess routine restricted transfers. Where a TRA indicates that there is a higher degree of risk, a more detailed assessment or other transfer tool will be required. This takes a more cautious approach than the EDPB Recommendations, which are quick to conclude that transfers should not take place where there is risk.

Ongoing compliance: If transfers under an IDTA are continuous and relate to an ongoing flow of data, organisations must regularly reassess the level of protection the IDTA provides as well as any extra steps or measures put in place to safeguard the data. The level of protection for the data must be maintained and ongoing assessments must ensure that the level of protection does not decrease over time. If there are any changes in the type of data being processed or the kind of processing being carried out by the processor or if the laws in the destination country change, organisations should update their TRA to ensure the transfer remains compliant.

Onward transfers: If an importer intends to make onward data transfers to third parties, organisations are obliged to consider how that secondary transfer complies with the IDTA, in the same way as the assessment for the initial transfer. If the importer will rely on an Article 46 transfer tool to make its onward transfer, then the exporter and importer of the initial transfer must make sure there is a TRA which covers that onward transfer of data.

What does the TRA tool do?

The aim of a TRA is to assess whether applicable local laws and practices of the recipient country of the personal data override the protections afforded by the IDTA. The outcome of the TRA is to help determine whether a restricted transfer may proceed solely on the basis of the IDTA, or if extra steps and protections may be required to legitimise the transfer.

Unlike under the EDPB Recommendations, a restricted transfer may potentially go ahead if the risk of harm to data subjects is low, even where disproportionate third-party access may occur. In this scenario, organisations would look to use the IDTA together with any extra steps and protections identified. If, however, no extra steps are likely to help, the fallback position would be to consider other transfer tools than the IDTA or the derogations under Article 49 of the UK GDPR.

Remember:

- You only need to consider those parts of the destination country's regime that are relevant to your restricted transfer.
- **There may not always be additional measures you can take to reduce the risk of harm to data subjects. If this is the case, the transfer cannot continue until changes to the transfer arrangements are made.**

The TRA sets out a three-step assessment method, which we summarise below:

Step 1 – assessing the transfer

As with the EDPB Guidance, the first step is to map out data flows, taking into account the specific details of transfers (such as categories of data, duration of transfer and the likelihood of onward transfer).

Initially, the TRA requires organisations to assess the specific circumstances of the transfer to identify those restricted transfers that may be too high risk or complex for the TRA tool. Some examples of where this might be the case are where multiple jurisdictions are involved or the transfer is to a destination country that has a poor human rights record.

This step also requires organisations to take into account the overarching UK GDPR requirements for continuing with a restricted transfer, such as transparency and data minimisation.

Step 2 – enforceability of the IDTA in the destination country

In line with *Schrems II*, the TRA makes it clear that organisations making restricted transfers to third countries need to undertake an assessment of the local laws in the destination country to understand whether the personal data will be afforded a "substantially similar" level of protection to that in the UK.

The TRA tool uses a set of tables to help make this assessment:

- Table A examines the enforceability of contractual safeguards in the destination country.
- Table B looks at the overall risks to data subjects in relation to the enforceability of the IDTA.
- Table C looks at measures to supplement the IDTA safeguards.

Based on the response to Table A, if the assessment of the recipient country laws does not contradict or derogate from the protections afforded under the IDTA, then the supplementary assessments in Tables B and C will not be required.

Step 3 – protection from third party access

As part of the assessment required by *Schrems II*, organisations are required to assess the regulatory regime for third party access to data in the destination country. The Guidance sets out a decision tree to assist organisations in identifying how similar the UK's regime regarding third party access is to the regime of the destination country.

The TRA tool provides three tables for identifying rules around third party access. These provide a framework for organisations to assess:

- The factors of the destination country's third-party access regime and whether it safeguards or undermines data subject rights.
- The likelihood of third-party access, taking into account all the circumstances of the transfer and the destination country's regime.
- The overall risk to the data subject (including consideration of any extra protection measures that could be taken to reduce the risk of harm).

A final table includes a non-exhaustive list of additional measures that could be used to reduce the risk of harm to the data subjects.

www.shlegal.com

STEPHENSON HARWOOD

BD1118-SSCs IDTA update-0921