Out with the old, in with the new? A first look at the proposed UK approach to IDTs

Victoria Hordern, Partner and Head of Data Privacy with Bates Wells, explores the changes set out in the ICO's proposed International Data Transfer Agreement

Victoria Hordern is the eLearning course designer for PDP's training session 'International Data Transfers'. For further information on the content and fees for this course, see www.pdptraining.com

Data protection professionals are still getting used to the new world order of *Schrems II* (C-311/18) and the revised EU Standard Contractual Clauses published in June 2021 (the 'EU SCCs'). Now, they will need to integrate the changes recently proposed by the UK Information Commissioner's Office on international data transfers from the UK.

As a result of Brexit, the UK needed to set out its position on Chapter V of the UK GDPR concerning international data transfers and indicate how closely it was going to track the EU approach. Clarity on the ICO's approach is even more needed given that the EU SCCs do not exempt exporters that are not subject to the EU GDPR, leaving UK exporters currently (and somewhat paradoxically) having to still rely on the old EU SCCs from 2004 and 2010.

The ICO's stated aspiration with its solution — to help all organisations to understand and comply with the complex requirements of the law around international data transfers — is laudable. However, unfortunately there are no quick and easy solutions, and the terminology and concepts involved in international data transfers can flummox many.

The published documents that form the ICO's consultation comprise the Consultation Paper, the draft UK Addendum to the EU SCCs, the draft International Data Transfer Agreement ('IDTA') and the draft International Transfer Risk Assessment and tool ('TRA') (copies of all are available via: www.pdpjournals.com/docs/888171). This article discusses each element of the consultation and highlights some of the likely compliance issues for organisations should the proposals make it into the final solution for international data transfers from the UK.

The Consultation Paper

The ICO indicates in the Consultation Paper that it will be updating its guidance on Chapter V and restricted transfers, as well as providing guidance on a TRA and publishing a final IDTA. The Consultation Paper seeks views on the draft IDTA and TRA. It also requests feedback on a number of technically complicated questions concerning the extra-territorial effect of Article 3 UK GDPR. It ask for responses on the positions under UK law of processors of a UK GDPR controller under Article 3(1), processors of a UK GDPR controller under Article 3(2) and an overseas joint controller with a UK-based joint controller. Additionally, the ICO has posed certain questions on the scope of Article 44 UK GDPR and when a restricted transfer takes place (a restricted transfer is a transfer to a third country which can only take place if Chapter V is complied with). For instance, the ICO proposes there is no restricted transfer if a UK company shares personal data with its overseas branch.

The Consultation Paper includes questions on the status of derogations under Article 49 and the use of the IDTA in conjunction with the derogations. It also indicates the likely timeline for the UK to disapply the use by UK organisations of the old EU SCCs (introduced under EU Data Protection Directive 95/46/EC and currently still available to rely on in the UK).

UK Addendum to EU SCCs

In some good news from the proposals, the ICO has provided a reasonably simple solution for organisations that are making data transfers from both the EU and the UK and wish to rely on the EU SCCs for both data transfers.

In such instances, an organisation can rely on a UK addendum (provided by the ICO in draft) to the EU SCCs where the UK addendum amends the EU SCCs to work in the context of UK data transfers. The addendum itself is mercifully short (four pages) and pretty straightforward to complete, although doubtless there are likely to be certain details from the EU SCCs which the simplicity of this solution will struggle with.

The ICO indicates that this approach — a UK specific addendum to sit alongside another model data trans-

(Continued on page 4)

(Continued from page 3)

fer agreement — is likely to be one that it explores for other data protection frameworks that issue model data transfer agreements, for example, the Association of Southeast Asian Nations. Certainly for global organisations that are routinely entering into agreements affecting operations in the UK and the EU, this solution is welcome.

The new International Data Transfer Agreement

The new procedures in the UK will bring in a change of terminology. No longer will we refer to the SCCs for international data transfers from the UK. The ICO has provided a draft International Data Transfer Agreement or IDTA.

The change in the name also indicates a change in format. The EU SCCs follow a modular approach — four modules to cover four different types of data transfers from the EU. The ICO has chosen not to follow this approach. Instead, the key provisions — Mandatory Clauses — indicate when certain clauses do or do not apply depending on the roles of the parties.

The IDTA is split into four parts:

Part One: Tables — This is where the parties describe themselves, details of the transfer, any Linked Agreement (e.g. Article 28 Agreement), types of data being transferred, the purpose of the transfer, and security requirements, etc.

"Certain aspects of the Mandatory Clauses in the IDTA appear to reflect a different approach to that set out in the EU SCCs. For instance, while the EU SCCs indicate that reliance on the EU SCCs can satisfy the requirements under Article 28 EU GDPR, the IDTA does not indicate the same with respect to Article 28 UK GDPR."

Part Two: Extra Protection Clauses: — This part is relevant when the TRA indicates that extra steps and protections are required to maintain the right level of protection in the IDTA (in other words, in EU terminology, introducing supplementary measures).

Part Three: Commercial Clauses — This part is only relevant if the parties need to add further clauses since commercial aspects may already be covered in Linked Agreements.

Part Four: Mandatory Clauses — These are the key clauses that are designed to mirror the SCCs approach, i.e. provide appropriate safeguards.

Certain aspects of the Mandatory Clauses in the IDTA appear to reflect a different approach to that set out in the EU SCCs. For instance, while the EU SCCs indicate that reliance on the EU SCCs can satisfy the requirements under Article 28 EU GDPR, the IDTA does not indicate the same with respect to Article 28 UK GDPR. Significantly, the IDTA is drafted so that even if the parties select erroneous transfer details in the Tables (i.e. describe the importer as a processor when they are a controller), the IDTA will still apply to the greatest extent possible. In other words, the IDTA sort of 'auto-corrects'.

Certain clauses in the IDTA reflect the same concerns of the EU SCCs. For example, where an importer is providing information regarding its local laws and practices which could impact on the transferred data, any additional clauses must not undermine the protection provided to personal data. However, the IDTA also includes new aspects: an arbitration provision for dealing with disputes, and a test of 'Significant Harmful Impact' where the importer is in breach of the IDTA. Anyone hoping that the ICO's IDTA would revert to a shorter and more simplistic approach than the EU SCCs will be disappointed (a consequence, at least in part, of how the law has developed).

While certain aspects of the IDTA are designed to increase flexibility for data transfers, it's also possible that departing from the EU SCCs approach could lead to more compliance headaches for UK organisations. Will global service providers with customers across the EU who are likely to adopt an approach to international data transfers based on the EU SCCs be willing to spend time negotiating the IDTA with UK customers, when only dealing with transfers from the UK for that customer (especially if they have only a few UK customers)?

The ICO's Transfer Risk Assessment

The ICO has underlined that due to *Schrems II*, there is now a requirement in the UK to complete a TRA before entering into the IDTA or making any other international data transfers when relying on appropriate safeguards (so relying on the UK Addendum to the EU SCCs, as well).

A TRA is not required when organisations are sending data to a country covered by UK adequacy regulations or where they are relying on a derogation (where there's even less protection for the data). Otherwise, a TRA is now a fact of life for all UK organisations involved in international data transfers. The TRA that the ICO has published will therefore be a key tool for UK organisations to rely on although, it's important to stress, that it is just one approach and organisations can choose to develop their own transfer risk assessments.

The ICO's TRA differs from the outline to a risk assessment indicated in the European Data Protection Board's ('EDPB') June 2021 recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Certain differences are cosmetic.

For instance, the EDPB outlines a roadmap with five steps, whereas the ICO uses three steps. Other changes are more significant, for instance that the TRA allows the exporter to place greater weight on the risk relevant to the type of data being transferred and the risk of harm to individuals in the third country. This could enable an exporter to reach different conclusions under the EDPB's model and the ICO's in carrying out a risk assessment for a particular transfer.

A strict reading of the EDPB recommendations would suggest that an EU exporter must never transfer personal data to a country where the law of that third country prohibits the supplementary measures the exporter has identified. It is arguable in light of the approach proposed in the TRA by the ICO that low risk data transferred from the UK to that third country whose use is highly unlikely to cause harm to those individuals could be transferred to that country, despite the prohibition.

The TRA's three-step roadmap approach within the transfer risk tool is assessing:

- the transfer itself;
- whether the IDTA likely to be enforceable in the destination country; and
- whether there appropriate protection for the data from third-party access

Under the first step, the exporter needs to consider whether the transfer satisfies the key requirements of the UK GDPR more generally, for example, requirements on data minimisation, security and identifying a lawful basis. The exporter should also consider whether the TRA is suitable for the proposed transfer and the specific circumstances of the restricted transfer. Significantly, the ICO indicates that there may be transfers that are so high risk and complex that the TRA is not suitable. Examples would be where the transfer requires a DPIA, the transfer involves use of new technologies or the third country where data are being transferred to has high risk human rights concerns.

In considering the second and third stages, the ICO has provided a series of tables to support organisations in determining the compliance steps and navigating the difficult legal issues. Within each table, the ICO has set out its view of the different parameters for low, moderate and high risk circumstances. For step two, the tables cover:

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

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

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

For step three:

Table D: Assessing third party access or surveillance regime

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

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

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

Consequently, a UK exporter seeking to adopt the TRA will need to allow for additional time and resources to complete and document the steps for each data transfer.

Certain evaluations will be quite new. For instance, under step three, the exporter is asked to consider whether the destination (or third) country's regime is similar enough to the UK's regime in terms of regulating third party access to data (including surveillance). This presupposes that the UK exporter has a working knowledge of the UK legal regime in this area in the first place.

Final remarks

It's undeniable that the law around international data transfers has become fiendishly more complex over the last 14 months. Organisations with both a UK and EU presence will need to keep an eye on developments and guidance in both the UK and the EU going forward. The opportunity to input into the UK's approach as outlined in the ICO's consultation runs until 7th October 2021.

Victoria Hordern, Partner at Bates Wells, is leading a Workshop on the 'Practical Implications of Using Standard Contractual Clauses' at the 20th Annual Data Protection Compliance Conference, taking place in London and virtually on 7th and 8th October 2021. See www.pdpconferences.com

Victoria Hordern
Bates Wells
v.hordern@bateswells.co.uk