PRIVACY & DATA PROTECTION VOLUME 26, ISSUE 4

From adequacy to TRAs: Decoding the ICO's latest international transfers guidance

Tim Hickman, Partner
Joe Devine, Associate
White & Case

Tim Hickman, Partner and Head of Data, Privacy & Cyber Security, and Joe Devine, Associate, White & Case, examine the ICO's published updated guidance on international transfers of personal data

Chapter V of the UK GDPR imposes a general prohibition on transfers of personal data from organisations in the UK to recipients located outside of the UK, unless the jurisdiction in which the data recipient is located benefits from an 'adequacy regulation', appropriate transfer mechanisms are implemented, or a derogation applies. To assist organisations with identifying when international transfers of personal data occur, and to help with understanding, navigating, and complying with the relevant rules, the UK Information Commissioner's Office ('the ICO') has published a detailed suite of new and updated guidance (the 'Guidance').

At a high-level, the Guidance provides information and direction to organisations on a range of topics, including:

- when the rules on transferring personal data to other countries apply, and who is responsible for complying with the rules;
- how to make a 'restricted transfer' of personal data;
- making transfers on the basis of 'adequacy regulations';
- transfer risk assessments ('TRAs'), including when organisations must complete TRAs; and
- relying on 'derogations' to transfer personal data internationally.

The ICO has said that it will continue to update the Guidance, including with respect to TRAs, the UK international data transfer agreement ('IDTA') and cloud services, and plans to add an interactive tool to assist organisations in determining whether they are making a restricted transfer, as well as provide further examples and case studies that reflect the complexity of global transfer scenarios.

This article summarises the key areas of the Guidance that are likely to impact organsiations. For organisations that are already closely familiar with Chapter V of the UK GDPR, the Guidance contains no major surprises, but is helpful for refreshing and clarifying the existing position.

The ICO's three-step test to determine whether a transfer is 'restricted'

The Guidance sets out a three-step test to assist organisations with determining whether a transfer of personal data will be 'restricted' under the UK GDPR. If the answer to all three questions is 'yes', the transfer is restricted.

Step 1: Does the UK GDPR apply to the relevant processing? The Guidance reminds organisations that the UK GDPR applies to entities that are: (i) established in the UK; or (ii) established outside of the UK, but that (a) offer

goods or services to data subjects in the UK, or (b) monitor the behaviour of data subjects in the UK.

Step 2: Is the information being sent to a recipient outside the UK? The Guidance explains that a 'transfer' includes making personal data accessible outside of the UK (e.g., allowing organisations to access systems remotely).

Step 3: Is the recipient a separate legal entity? If the sender and the recipient are the same legal entity, there is no transfer.

Practical case studies of restricted transfers

The Guidance provides examples to illustrate when 'restricted' transfers occur under the UK GDPR. For example, the Guidance clarifies that where: (i) a UK organisation permits a non-UK organisation (e.g., an IT service provider in India) to remotely access personal data stored on the UK organisation's servers; (ii) a UK organisation transfers personal data to a cloud services provider established outside the UK (e.g., a customer resource management service provider in the USA); or (iii) a UK organisation transfers personal data to a group company located outside the UK (e.g., in China), a restricted transfer is taking place in each case.

Notably, the ICO's position in this regard diverges from the analogous EU GDPR position'

The Guidance also provides examples to illustrate when 'restricted' transfers do not occur under the UK GDPR. For example, the Guidance clarifies that a UK-based processor that provides services to a controller located outside the UK will not be making a restricted transfer when transferring data back to the controller, provided that the processor: (i) only handles the personal data as a processor under the instructions of the controller; and (ii) transfers the same personal data back to the same controller that instructed the processor to carry out the processing. Notably, the ICO's position in this regard diverges from the analogous EU GDPR position. The European Data Protection Board (the 'EDPB') takes the view that a transfer of personal data from an EEA-based processor back to a controller located outside of the EEA amounts to an international transfer that must be protected in accordance with Chapter V of the EU GDPR. (See examples 6 & 10 of the EDPB's Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.)

Indeed, Module 4 of the EU Standard Contractual Clauses (the 'EU SCCs') (i.e., a set of template contractual terms that have been approved by the European Commission (the 'Commission') to safeguard personal data transferred to recipients outside of the EEA) is specifically designed to facilitate and protect transfers of personal data from EEA-based processors to non-EEA controllers.

The EU Commission FAQs on the EU SCCs provide the following two examples of when Module 4 may be used by EEA-based processors:

> *"A Moroccan company uses cloud services offered by a Luxembourg company to manage its customer database. The [EU] SCCs (Module 4) can be used by the Luxembourg company (the data exporter) to transfer the data from its server in Luxembourg (back) to the Morocco client (the data importer)."*

> *"A university in Tunisia hires a research institute in Belgium to carry out a survey for which it collects and processes data in the EU and sends it to the university. The [EU] SCCs (Module 4) can be used by the Belgian institute (the data exporter) to transfer the data to the university in Tunisia (the data importer)."*

Arguably, the ICO takes a more pragmatic approach to data protection compliance in this context. Service providers with operations in both the EU and the UK that provide services (as processors) to non-EEA / non-UK customers (i.e., which are

controllers when receiving such services) should keep in mind that the relevant compliance obligations differ under the EU GDPR and UK GDPR in this regard.

Roles and responsibilities

The Guidance makes it clear that responsibility for complying with Chapter V of the UK GDPR rests with the party that 'initiates' the restricted transfer, i.e., the party that chooses to make the transfer happen as part of their processing purposes or service delivery. The Guidance cites the following factors as 'simple indicators' of whether an organisation is 'initiating' a transfer:

- a controller transferring personal data to a processor located outside the UK is initiating the transfer;
- a processor located in the UK transferring personal data to a sub-processor located outside the UK is initiating the transfer; and
- a controller that instructs processor A to transfer personal data to processor B is initiating the transfer (even where the transfer itself is carried out by processor A, rather than the controller). For example, if a UK-based controller instructs a UK-based processor to transfer personal data to a separate processor located in Mexico, the UK controller is initiating the restricted transfer to the Mexican processor, and therefore the UK controller bears primary responsibility for compliance with Chapter V of the UK GDPR.

UK adequacy regulations

The Guidance includes detailed information on how UK adequacy works, and provides specific guidance on the UK Extension to the EU-US Data Privacy Framework (which allows transfers of personal data from the UK to US organisations that are certified to the EU-US Data Privacy Framework).

As noted above, Chapter V of the UK GDPR permits transfers of personal data (without the need for additional transfer mechanisms) to jurisdictions that are deemed to have an 'adequate' level of protection for transferred personal data (i.e., an 'adequacy regulation'). The Guidance explains that:

- adequacy regulations are either 'full' (e.g., for a specified country) or 'partial' (e.g., for a sector, specific categories of personal data, or specific conditions apply, etc.), and that before relying on partial adequacy regulations, organisations should check the scope of the relevant adequacy regulation(s) and ensure that they cover the proposed transfer. The Guidance sets out a summary of full and partial adequacy regulations; and
- organisations do not need to complete a TRA or put in place other appropriate safeguards where an adequacy regulation applies, but organisations should still make reasonable and proportionate checks to confirm that the recipient will comply with its data protection obligations under local data protection laws.

For completeness, an adequacy regulation does not affect Article 28 of the UK GDPR. This means that, where a controller in the UK engages a processor in an 'adequate' jurisdiction, there is no need for a transfer mechanism (as explained above), but the controller still needs to implement a processing agreement in accordance with Article 28 UK GDPR.

Appropriate safeguards and TRAs

If an adequacy regulation does not apply, the restricted transfer must be protected by one of the appropriate safeguards listed in Article 46 of the UK GDPR (e.g., an IDTA). Before relying on one of these safeguards, an organisation must first complete a TRA to ensure that the standard of protection for the transferred personal data will not be 'materially lower' post-transfer.

The Guidance explains what a TRA is, when one is required, who is responsible for completing a TRA, and how to complete it.

When a TRA is required: An organisation must complete a TRA if it: (i) initiates a restricted transfer; and (ii) intends to rely on an appropriate safeguard to make the restricted transfer.

Who needs to complete the TRA: The Guidance clarifies that the entity 'initiating' the restricted transfer will be responsible for completing the TRA. As discussed above, the party that 'initiates' a restricted transfer may be a controller or a processor.

How to complete a TRA: The Guidance explains how to complete TRAs, including the types of risks that should be considered and addressed.

The ICO has also created a new optional, interactive TRA tool that is designed to help guide organisations through completing TRAs, and to help organisations evaluate risks associated with intended transfers, and whether chosen safeguards provide adequate protection to personal data.

IDTA and Addendum

The Guidance confirms that organisations may incorporate the IDTA Part 4 mandatory clauses into contracts by reference (i.e., as opposed to restating these in full), and provides specific language that must be included where an organisation chooses to take this approach.

The Guidance similarly confirms that organisations may incorporate the Part 2 mandatory clauses of the International Data Transfer Addendum (the 'Addendum') into contracts by reference. As a reminder, the EU SCCs are not valid for restricted transfers under the UK GDPR without the Addendum.

In each case, this will come as welcome news to organisations that intend to rely on the IDTA or the Addendum to make restricted transfers. Practically speaking, this will enable organisations to materially cut the length of commercial contracts that involve international transfers of personal data, and that incorporate the IDTA or the Addendum.

Although many organisations choose to incorporate the EU SCCs by reference (i.e., to save restating the EU SCCs in commercial contracts in full), the Commission FAQs are silent on whether this approach is compliant.

Other key UK GDPR obligations in the context of international transfers

The Guidance includes an updated section that reminds organisations of their wider UK GPDR obligations in the context of international transfers of personal data (i.e., obligations beyond Chapter V of UK GDPR). For example, the Guidance reminds controllers that they must ensure that:

- the restricted transfers comply with the data protection principles of Article 5 UK GDPR;
- the restricted transfers have a lawful basis Article 6 UK GDPR;
- data subjects are informed about restricted transfers of their personal data under Article 12 UK GDPR;
- the restricted transfers are recorded in Article 30 UK GDPR records of processing activities; and
- appropriate technical and organisational measures are in place to ensure that restricted transfers are made securely in accordance with Article 32 UK GDPR.

The Guidance also sets out recommendations regarding onward transfers of personal data. In particular, the Guidance directs organisations to consider whether recipients of data are likely to further transfer that data and, if so, what practical steps could be taken by UK organisations to reduce risks to data subjects in that regard. In particular, organisations should map all possible onward transfers and take steps to implement the ICO's recommendations to:

- reduce or pseudonymise personal data transferred to non-UK controllers;
- review copies of the receiver's contracts or risk assessments for onward transfers;
- require additional audits or checks of the recipient's processing and onward transfers in a contract (including copies of the receiver's contracts or risk assessments for onward transfers);

- prohibit or impose conditions on any onward transfers in contracts with the recipient; and
- consider whether any contractual limits of liability are sufficient, where relevant and appropriate.

Conclusion

Organisations should:

1. Continue to monitor the ICO's website for new guidance (this journal will be tracking the developments closely and reporting on updates);
2. Map out their data flows and apply the ICO's three-step test to determine whether any transfers of data are 'restricted' under the UK GDPR;
3. Check adequacy regulations and consider the availability of appropriate safeguards to protect any restricted transfers;
4. Where no adequacy regulations apply, conduct a TRA and implement safeguards before initiating restricted transfers of personal data;
5. Consult the ICO's TRA tool when completing TRAs for restricted transfers; and
6. Map all possible onward transfers, and take steps to reduce risk where relevant and appropriate

The authors would like to acknowledge Emily Digby for her work on this article.

Tim Hickman | tim.hickman@whitecase.com
Joe Devine | joe.devine@whitecase.com
White & Case