The IAF submitted the following comments to the Information Commissioner of the United Kingdom under question 9 of the ICO consultation on "international Transfers under the UK GDPR"

The Information Accountability Foundation (IAF), a non-profit research and education think tank, appreciates the opportunity to submit comments on Section 2 of the ICO's Consultation on International Transfers under the UK GDPR (Consultation). The IAF's mission is collaborative scholarship and education on the policies and processes necessary to use data responsibly in an observational age, while enabling a trusted digital ecosystem that serves people. IAF scholarship is based on three core beliefs:

- To enable and achieve the benefits of a global digital ecosystem, organizations must be able to think with data and engage in knowledge discovery and creation.
- To be trusted, organizations must be accountable, responsible, and answerable and be prepared to demonstrate their accountability.
- To enable beneficial, data-driven innovation while protecting individuals and society from the potential harms that may arise from data processing in the digital age, frameworks must be based on risk assessments and effective and risk appropriate data governance.

These views reflect the views of IAF staff and do not necessarily reflect the views of the IAF board of trustees, contributors, or broader community.

Background

The IAF's core beliefs match up with the reasons given by the Department for Digital, Culture, Media & Sport (DCMS) regarding why international data transfers are important in its August 2021 Guidance on International data transfers: building trust, delivering growth, and firing up innovation (Guidance). As set forth in the Guidance, international data transfers:

- Drive international commerce, trade, and development
- Underpin innovation, research, and development across multiple sectors
- Support international cooperation
- Enable us to stay emotionally and socially connected to one another

With respect to alternative transfer mechanisms, the Guidance states that the UK government is working with the ICO to ensure that UK businesses, and third and public sector organisations, have effective and economical mechanisms that provide appropriate safeguards for transferring personal data internationally. These mechanisms are to continue to be supported by clear and pragmatic guidance which enables UK data controllers of all sizes to implement them.

Summary of IAF Findings

The IAF staff believe the draft transfer risk assessment (TRA) is not consistent with the objectives put forward by DCMS because it requires parties transferring data from the UK to a third country to conduct a full adequacy assessment which is beyond what is required by Schrems II and because it goes beyond the guidance put forward by the European Data Protection Board (EDPB).

Question 9 of Section 2 of the Consultation: Transfer risk assessments.

Q9. Please provide us with your views on the draft TRA tool, in particular:

- Do you consider it practical? Do you have any suggestions about how we could make it more helpful?
- Do you agree with the underlying decision tree and our approach to risk?
- Do you agree that the IDTA may be used where the risk of harm to data subjects is low?

The Draft TRA

The TRA asks the data exporter to:

- Step 1: Evaluate whether the transfer meets the key UK GDPR requirements, including whether if the importer was in the UK, would it comply with UK GDPR Article 6 lawfulness of processing and whether data subjects have been made aware of the processing that is taking place through appropriate privacy notices. If the answer is No, then the transfer cannot proceed; if the answer is Yes, then the data exporter proceeds to Step 2.
- Step 2: Assess whether the contractual safeguards are likely to be enforceable in the destination country. If the answer is No or Don't Know and so serious risks are assumed, then the risk of harm to individuals is assessed taking into account the specific circumstances of the transfer and any concerns about the destination country's regime. If extra steps and protections can be taken to reduce the risk to low or the risk is low, then the data exporter proceeds to Step 3. If extra steps and precautions cannot be taken, then the transfer cannot proceed.
- Step 3: Assess whether the destination's country's regime is similar enough to the UK's regime in terms of regulating third party access to data (including surveillance). If it is similar enough, the transfer can proceed. If the answer is No or Don't Know and so serious concerns are assumed, then assess how likely it is

that third parties (i.e., public authorities and private companies) have access to the data (including surveillance). If minimal risk, the transfer can proceed. If the answer is more than minimal risk or don't know and so more than minimal risk is assumed, then what the risk of harm is considering the circumstances of the transfer and the destination country's regime is considered. If the risk is low, then the transfer can proceed. If extra precautions can be taken to reduce the risk of harm to low risk, then the transfer can proceed; if extra precautions cannot be taken or they do not reduce the risk, then the transfer cannot proceed.

The TRA is more rigorous than what is required by Schrems II and by the EDPB's Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (EDPB Final Recommendations) and so are impractical and do not facilitate international data transfers. Rather, the TRA takes an approach more similar to determining whether the third country provides an adequate level of protection. How to make that determination is set forth in the Article 29 Working Party's Adequacy Referential (Referential).

The Referential

The Referential sets forth the basic content and procedural/enforcement data protection principles and mechanisms a third country's system must contain. Examples of these content principles are:

- Basic data protection concepts and/or principles should exist. They do not have to mirror the EU GDPR terminology but should reflect and be consistent with the concepts in European data protection law.
- Lawful, fair, and legitimate principle. Data must be processed in a lawful, fair, and legitimate manner.
- Data quality and proportionality principle. The data should be adequate, relevant, and not excessive in relation to the purposes for which they are processed.
- Security and confidentiality principle. Any entity processing personal data should ensure that data are processed in a manner that ensures security of the data using appropriate technical or organisational measures.
- Transparency principle. Each individual should be informed of all the main elements of the processing of his/her personal data in a clear, easily accessible, concise, transparent and intelligible form.

Like the Referential, the TRA asks whether the key requirements under the UK GDPR can be satisfied. The TRA states that the transfer should not be made without ensuring that, in addition to the international transfer rules, it meets the rest of the UK GDPR requirements. According to the TRA, the fundamental principles set out in Article 5 of the UK GDPR (lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; accountability) must be satisfied, and if the processing does not meet these requirements, then the transfer cannot go ahead (and the transfer questions do not even need to be considered).

The TRA gives the following as examples of key requirements that should be checked:

- data minimization – are the data to be transferred adequate, relevant, and limited to what is necessary
- security – have technical and organizational measures to ensure a level of security appropriate to the risk been put in place
- lawful basis - is the transfer of data fair and lawful
- transparency – have data subjects been made aware through appropriate privacy notices of the processing that is taking place

Another example of how the TRA goes too far is in Step 3 where the TRA asks about third party access to data (including surveillance) and defines third parties as including public authorities and private companies. As discussed below, Schrems II makes it very clear that one of the factors to be considered is the access of public authorities in the third country to personal data transferred to the third country.

Schrems II and the EDPB's Final Recommendations

In Schrems II, the European Court of Justice (ECJ) was asked to specify which factors need to be taken into consideration for the purpose of determining whether the level of protection required by Articles 46(1) and 46(2)(c) of the EU GDPR is ensured in the context of transfer of personal data to a third country based on standard data protection clauses. Before answering this question, the ECJ reviewed the applicable provisions of the EU GDPR:

- In the absence of an adequacy decision under Article 45(3) of the EU GDPR, a controller or processor may transfer personal data to a third country only if: (i) the controller or processor has provided appropriate safeguards (e.g., standard data protection clauses adopted by the European Commission), and (ii) enforceable data subject rights and effective legal remedies for data subjects are available.
- Although Article 46 of the EU GDPR does not specify the nature of the requirements which flow from the reference to "appropriate safeguards," "enforceable rights," and "enforceable remedies," because Article 46 appears in Chapter V of the EU GDPR, it must be read in light of Article 44 of the EU GDPR. Article 44 is entitled "General principle for transfers" and provides that "all provisions [in that chapter] shall be applied in order to ensure that level of protection of natural persons guaranteed by [the EU GDPR] is not undermined."
- In the absence of an adequacy decision, the appropriate safeguards to be taken by the controller or processor in accordance with Article 46(1) of the EU GDPR must compensate for the lack of data protection in a third country in order to ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the EU.

After reiterating the question, what factors should be taken into consideration for the purposes of determining the adequacy of the level of protection where personal data is transferred to a third country pursuant to standard data protection clauses adopted under Article 46(2) of the EU GDPR, the ECJ answered as follows:

- Although Article 46(2) of the EU GDPR does not list the various factors which must be taken into consideration for the purposes of assessing the adequacy of the level of protection to be observed in such a transfer, Article 46(1) of the EU GDPR states that data subjects must be afforded appropriate safeguards, enforceable rights, and effective legal remedies.
- The assessment required for that purpose in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the EU and the recipient of the transfer established in the third country and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country. As regards the latter [access by the third country's public authorities to the personal data transferred], the factors to be taken into consideration in the context of Article 46 of the EU GDPR correspond to those set out, in a non-exhaustive manner, in Article 45(2) of the EU GDPR:
    - The rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules, and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
    - The existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
    - The international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relations to the protection of personal data.
- Therefore, the assessment of the level of protection afforded in the context of a transfer of personal data to a third country pursuant to standard contractual clauses must, in particular, take into consideration both the contractual clauses between the controller or processor established in the EU and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of the EU GDPR.

Although Schrems II sets forth the factors that should be taken into consideration for the purposes of determining the level of protection where personal data is transferred to a third country pursuant to standard data protection clauses, the same factors should apply to the other appropriate safeguards in Article 46 of the EU GDPR (legally binding and enforceable instrument between public authorities or bodies, binding corporate rules, standard data protection clauses adopted by a supervisory authority and approved by the European Commission, approved code of conduct, and approved certification method) because they are contractual in nature as well.

The EDPB's Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (EDPB Final Recommendations) provide in Step Three that the data exporter in collaboration with the data importer should assess if there is anything in the law and/or practices in force in the third country that may impinge on the effectiveness of the appropriate safeguards of the EU GDPR Article 46 transfer tool relied on in the context of the specific transfer.

- This assessment must be based on legislation publicly available and must address access to data by public authorities of the importer's third country. Examining the practices in force in the third country is especially important in the assessment of the following situations:
    - Practices of public authorities (e.g., accessing personal data held by the private sector or when enforcing -or not- legislation as supervisory or judicial bodies) may clearly indicate that they do not normally apply/comply with the legislation that governs, in principle, their activities.
    - Relevant legislation in the third country (e.g., on access to personal data held by the private sector) may be lacking.
    - Relevant legislation in the third country might be problematic and transferred data and/or the importer fall or might fall within the scope of the problematic legislation.
- The scope of the assessment is limited to the legislation and practices relevant to the protection of the specific data transfer, in contrast with the general and wide encompassing adequacy assessment the European Commission carries out in accordance with Article 45 of the EU GDPR. Specific attention should be paid to relevant laws, in particular laws laying down requirements to disclose personal data to public authorities or granting to public authorities powers of access to personal data (e.g., criminal law enforcement, regulatory supervision, or national security purposes). If these requirements or powers restrict the fundamental rights of data subjects while respecting their essence and being necessary and proportionate in a democratic society to safeguard important objectives as also recognized in EU or EU Member States' law, they may not impinge on the commitments contained in the EU GDPR Article 46 transfer tool being relied on.
- Documented practical experience of the importer with relevant prior instances of requests for access received from public authorities in the third country may be taken into consideration. The experience of the importer will be able to be used only if the legal framework of the third country does not prohibit the importer from providing information on requests for disclosure from public authorities or on the

absence of such requests. The absence of prior instances of requests received by the importer can never be considered, by itself, as a decisive factor on the effectiveness of the EU GDPR Article 45 transfer tool that allows the transfer to proceed without supplementary measures. This information will be able to be considered, together with other types of information obtained from other sources, as part of the overall assessment of the laws and practices of the third country in relation to the transfer.

Thus, the questions that the TRA should be asking are limited to: (1) what enforceable data subject rights exist in the third country, (2) what effective administrative and judicial redress is available to data subjects if their personal data transferred to a third country is subject to access by public authorities in that third country, and (3) does any legislation in the third country impinge on the appropriate safeguard. Simplifying the TRA to these three subject areas would make the TRA more helpful because it would focus on the issues pertinent to the transfer and this focus would make the TRA more practical.

The idea of a decision tree is very helpful both visually and conceptually, and the focus on high-risk areas makes sense. As discussed above, the decision tree must be revised so that the assessment contained in the decision tree is the more narrow assessment required by Schrems II. Specifically:

- Table A (Enforceability of contractual safeguards in the destination country) is consistent with Schrems II.
- Table B (Assessing overall risks to data subjects arising from the specific circumstances of the transfer, caused by concerns over the enforceability of the IDTA (the UK's version of the SCC)) and Table F (Assessing the overall risk of harm to data subjects arising from the specific circumstances of the transfer caused by third party access) focus on low, moderate, and high risk make them very confusing, especially for small and medium size businesses. Simplifying the tables to determine whether the risk is minimal or more than minimal so they match up with the decision tree would make them less confusing.
- Tables C and G (Types and levels of measures to supplement the IDTA safeguards) are very weak versions of the EDPB Final Recommendations; they should be strengthened by providing more examples.
- Table D (Assessing the third-party access or surveillance regime) and Table E (Assessing the likelihood of third-party access or surveillance) go too far because they cover both private companies and public authorities; according to Schrems II, the analysis should be limited to public authorities.

<u>Conclusion</u>

The transfer impact assessment called for by Schrems II and by the EDPB's Final Recommendations is not an adequacy assessment. Rather, the transfer impact assessment takes into consideration: (1) the appropriate safeguards, and (2) enforceable rights and effective legal remedies. Enforceable rights and remedies are assessed by looking at the relevant aspects of the legal system of the third country to determine whether public authorities of the third country can access the personal data transferred. What comprises

the relevant aspects of the third country's legal system is set out in a non-exhaustive manner in Article 45(2) of the EU GDPR.

The IAF appreciates this opportunity to submit comments on Section 2 of the Consultation. If you have questions, please contact Lynn Goldstein @ lgoldstein@informationaccountability.org.