IRSG RESPONSE TO THE ICO'S CONSULTATION ON INTERNATIONAL TRANSFERS UNDER UK GDPR

The IRSG is a practitioner-led body of leading UK-based representatives from the financial and professional services industry. It is an advisory body to the City of London Corporation, and to TheCityUK. The IRSG develops its policy positions through a number of workstreams which comprise representatives from across the financial services industry to ensure a cross-sectoral response.

To respond to the UK Information Commissioner's ("**ICO**") consultation on international transfers, it is necessary to download and complete the ICO's consultation paper.

For ease of tracking changes, we set out below draft responses to the ICO's proposals and welcome the comments of IRSG members. After the response is final, we will submit the response in the form required by the ICO.

The consultation is split into three sections, considered in turn below. It is not necessary to respond to all the questions.

Section 1: proposal and plans for the ICO to update its guidance on international transfers

A. Interpretation of extra-territorial effect of Article 3 UK GDPR

Proposal 1: Processors of a UK GDPR Controller under Art 3(1) UK GDPR

Q1: The ICO guidance requests that responders to the consultation select one of the following options:

- **Option 1- Processor of a UK GDPR is always covered by Art 3(1) UK GDPR:** This is based on an analysis that a processor of a UK GDPR controller is processing on behalf of its controller and so will inevitably be processing in the context of the UK GDPR controller's establishment.

- **Option 2 – whether the processor of a UK GDPR controller is covered by UK GDPR Art 3(1) is fact specific:** If the intention was that all processors of UK GDPR controllers were covered by UK GDPR, this would be expressly stated in UK GDPR. The decision in Google Spain was made based on the very specific facts of the case, and does not apply more broadly.

IRSG Response: Option 2. We agree with the ICO's preference for "Option 2". Article 3(2) UK GDPR determines the extra-territoriality of the UK GDPR. Our view is that if the intention was that all processors of UK based controllers were subject to the UK GDPR then that would be expressly stated in Article 3(2) UK GDPR. It would be unhelpful for the ICO to seek to expand the extra-territorial effect of the UK GDPR through its guidance to apply to processors of a UK controller *in all cases*. It is also questionable what public policy such a position would serve as even where on the specific facts of an individual case the processor is not directly subject to the UK GDPR, both data subjects and the ICO would continue to be able to exercise their rights against and regulate the UK based controller in the UK without having to deal with the complexities of enforcing remedies against a processor outside of the jurisdiction of the UK.

We request that the ICO adopts a position which is consistent with the European Data Protection Board ("**EDPB**") Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), which provides that the existence of an establishment should not be interpreted too broadly. The EDPB recommends a case by case analysis of each fact pattern, which we request that the ICO replicates this approach in its final form guidance. Inconsistency between the ICO and EDPB guidelines with regards to the scope of the GDPR would be unhelpful for entities with UK and EU operations.

Proposal 2: Processors of a UK GDPR Controller under Art 3(2)

Q2: The ICO guidance requests that responders to the consultation select one of the following options:

- **Option 1 - The processor of an Article 3(2) controller is also subject to UK GDPR by virtue of UK GDPR Art 3(2):** If the processing activities of the overseas controller are covered by UK GDPR Art 3(2), any processor carrying out those processing activities on behalf of its controller must also be covered by Article 3(2) UK GDPR. This is because the processor is carrying out processing relating to the controller's targeting or monitoring activity.

- **Option 2 - whether the processor of an Article 3(2) controller is also subject to UK GDPR pursuant to Article 3(2) UK GDPR will always depend on the circumstances**: The processor's processing activities will not always **relate to** the controller's targeting or monitoring activity. If the intention was that Art 3(2) would always apply to a processor if Article 3(2) applied to its controller, this would need explicit language in UK GDPR

IRSG Response: Option 2. Although we tend to agree that in most cases where a processor is processing on behalf of a controller caught by Article 3(2) GDPR it is likely that the processing will also be related to the activities triggering the application of Article 3(2) this may not always be the case and as noted in the consultation if this had been the intent then there would have been explicit language to this effect. If GDPR is determined on the particular circumstances *not* to apply directly to the processor, data subjects would nevertheless enjoy protection under Article 28 so there is no compelling public policy to take a binary position as proposed in Option 1.

Proposal 3: Overseas joint controller with a UK-based joint controller

Q3: The ICO guidance requests that responders to the consultation select one of the following options:

- **Option 1: An overseas joint controller with a UK based joint controller is always covered by Article 3(1) UK GDPR** - Controllers become joint controllers where they jointly determine the purposes and means of a processing activity. The UK controller is carrying out those processing activities in the context of its UK establishment (and so Art 3(1) applies). The overseas joint controller's processing activities (in light of being jointly determined) will inevitably be in the context of the UK GDPR controller's UK establishment.

- **Option 2**: **Whether the overseas joint controller is covered by Article 3(1) UK GDPR will always depend on the circumstances**. If the intention was that all overseas joint controllers with a UK-based joint controller must be covered by UK GDPR, this would be expressly stated in UK GDPR.

IRSG Response: Option 2. We agree with the ICO's preference for Option 2. Our view is that if the intention was that the UK GDPR would always apply to an overseas joint controller with a UK joint controller this would be explicitly stated in the UK GDPR. Having a joint controller relationship with a UK controller should not automatically give rise to the applicability of the UK GDPR.

By way of example, a UK based entity and an entity wholly based in the USA decide to host a virtual combined corporate networking event (B2B) primarily for corporate clients in the USA. Both parties design a portal for registration and determine what personal data they need to run the event. After an individual registers for the event, they will share their personal data with both entities and both entities will have access to a list of attendees. After the event, the parties jointly determine which entity would be best placed to follow up with particular corporate clients. It does not follow in this scenario that the USA based entity will be directly subject to the UK GDPR as it is not processing personal data in the context of a UK establishment (indeed, it does not have a UK establishment).

Selecting Option 1 (that the overseas controller is always covered by UK GDPR Art 3(1)) risks deterring collaboration among UK controllers and controllers in third countries at a time when the UK government is seeking to encourage an active and engaged global Britain.

B. Interpretation of Chapter V UK GDPR

Q4: The ICO guidance seeks (and IRSG is able to provide) input on:

Proposal 1: In order for a restricted transfer to take place, there must be a transfer from one legal entity to another (comments to be provided via free text) i.e. it would not be a restricted transfer where data flows within a legal entity (e.g. UK Company shares data with its overseas branch / employee takes laptop outside of the UK). Where the data flow stays within a single legal entity, it would still have to ensure those data flows comply with general UK GDPR obligations (eg security requirements) but not the transfer requirements in Chapter V.

IRSG response: We would welcome the final ICO guidance to adopt the position that in order for a restricted transfer to take place, there must be a transfer from one legal entity to another. To require entities to put in place Chapter V protections for intra-entity processing would put an unduly restrictive administrative burden on organisations and would be of questionable benefit to data subjects where the legal entity is in any event subject to the "full fat" application of GDPR.

We are aware that the supervisory authorities of some EU Member States may take a more restrictive view that Chapter V *does* apply to intra-entity transfers and to that end we would also welcome clarification in the final ICO guidance as to how to put in place SCCs where the exporter and importer are one in the same legal entity – where an exporter wishes to put in place protections notwithstanding the ICO's interpretation that intra-entity transfers are not restricted transfers. A deed poll may be a potential solution in these circumstances. It would be helpful if the ICO's final guidance permitted both options.

Proposal 2: A UK GDPR processor with a non-UK GDPR controller, will only make a restricted transfer to its own overseas sub-processors (comments to be provided via free text).

Q5: There is only a restricted transfer when the underlying decision to make the transfer is governed by UK GDPR. This interpretation means that:

- it is a restricted transfer when a UK GDPR processor (with a non-UK GDPR controller) appoints an overseas sub-processor and transfers personal data to it (Art 28(2) applies to that UK GDPR processor's decision to appoint its sub-processor); but
- it is not a restricted transfer when a UK GDPR processor (with a non-UK GDPR controller):
    - returns data to its non-UK GDPR controller; or
    - sends it on to a separate overseas controller or processor (but not its own sub-processor).

IRSG response: we welcome this helpful interpretation which will help to ensure as a matter of public policy that non-UK GDPR Controllers are not deterred from contracting with UK GDPR processors by requirements for additional SCCs to paper "reverse transfers" and by the threat of service interruption in the event the UK GDPR processor elected or was required by the ICO to suspend the transfer for any reason. The latter risks wider regulatory challenges for the non-UK GDPR controller to the extent they are in a sector requiring business continuity and disaster recovery planning as a condition of their authorisation. [Add idea to extend carve-out to all sub-processors where the controller in a third country has no nexus to UK; but this would require primary legislation – linkage to DCMS consultation.]

Proposal 3: Whether processing by the importer must not be governed by UK GDPR, for a transfer to be a restricted international transfer.

Q6: The ICO guidance requests that responders to the consultation select one of the following options:

- **Option 1 (ICO's current guidance)** - A restricted transfer only takes place where the importer's processing of the data is not subject to UK GDPR. If the importer is already required to process the data in accordance with UK GDPR, no additional Chapter V protection is needed. The ICO will have oversight of the importer's processing under UK GDPR and data subjects will have UK GDPR rights.
- **Option 2 (ICO updates guidance)** – Restricted transfer takes place whenever the exporter is subject to UK GDPR and the importer is located outside of the UK. It is not relevant whether or not UK GDPR applies to the importer. This option has the benefit of being more closely aligned to the language of Art 44.

IRSG response: We would welcome the ICO maintaining its current position whereby a restricted transfer only takes place where the importer's processing of the data is not subject to UK GDPR.

The purpose of Chapter V UK GDPR is to provide protection for data subjects in the event a recipient is subject to privacy legislation which offers less protection for personal data than the UK GDPR. . The ICO will have oversight of the importer and data subjects will have the "full fat" UK GDPR data subject rights, which in our view offers an appropriate level of protection. The analysis is very similar to the scenario covered by Question 4 above (intra-entity transfers where the entity is subject to the UK GDPR there is no need for the protections in Chapter V to apply).

Proposal 4: Proposal 4: Article 49 Derogations [add systemic or regular transfers comment – not just for ad hoc transfers except for the second hanging indent.]

Q7: The ICO is seeking views (via free text) regarding derogations and in particular:

- Should exporters first try to put an appropriate safeguard in place before relying on an Article 49 UK GDPR derogation?
- Should the requirements for those derogations to be "necessary" be interpreted as "strictly necessary"?

IRSG response: We would support guidance that exporters should *where reasonably practical* seek to implement appropriate safeguards under Article 46 of the UK GDPR reflecting the settled "waterfall" approach of the regulations in Chapter V and assuming that the export in question is not to a third country benefitting from an adequacgy decision. What would also be helpful would be for the guidance to acknowledge that implementing appropriate safeguards is often not possible through no fault of the exporter. Some types of importers such as regulators invariably refuse to sign up to any form of Article 46 appropriate safeguards. We are grateful to the ICO for its recent analysis on transfers from UK exporters to the US Securities and Exchange Commission which is just one example where regulators in third countries are currently not willing to implement Article 46 safeguards. Where this is the case and where the third country does not benefit from an adequacy decision then Article 49 is the *only* basis on which transfers may take place. Curtailing Article 49 for example by creating a condition that the exporter must be able to evidence the steps it has taken to try to implement Article 46 safeguards would risk creating a legal vacuum. Paragraph 200 of the CJEU's ruling in *Schrems II* is instructive on this point: *"As to whether it is appropriate to maintain the effects of that decision for the purposes of avoiding the creation of a legal vacuum (see, to that effect, judgment of 28 April 2016, Borealis Polyolefine and Others, C-191/14, C-192/14, C-295/14, C-389/14 and C-391/14 to C-393/14, EU:C:2016:311, paragraph 106), the Court notes that, in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR."* [Consider whether we can go further and drop any concept of the waterfall approach at all and allow exporters to go straight to Article 49 without having to consider Article 46 first. Potentially a stretch given well-settled guidance on the waterfall approach and also questionable public policy given more limited protections offered by Article 49.]

Regulators are just one example of importers who may be unwilling to implement Article 46 appropriate safeguards. Many government agencies, international bodies and commercial

counterparties are also reluctant to enter into standard contractual clauses or other appropriate safeguards. While on the one hand we accept that exporters must have responsibility to try to implement Article 46 appropriate safeguards as doing so requires the cooperation of third party importers, it would not be appropriate to prevent exporters from relying on an Article 49 derogation where an Article 46 appropriate safeguard is in theory available but not practical to implement.

As a matter of law we do not interpret Article 49 to include a requirement that as a pre-condition to rely on Article 49 either that a) no Article 46 safeguard is available for that transfer; *or* b) an Article 46 safeguard is available and the exporter has to be able to document that it has taken appropriate and proportionate steps to seek to implement the safeguard (unsuccessfully). Had such conditionality been intended, it would have been explicitly stated in Article 49. It was not.

It follows that if the ICO is considering including guidance on what steps exporters need to be able to demonstrate they have taken to comply with Article 46 in order to be able to satisfy the accountability principle (Article 5(2)) we request that the ICO clarifies in the guidance that while failing to be able to demonstrate the steps taken may amount to an infringement of Article 5(2) such failure would not prevent the exporter from relying on an Article 49 derogation.

We do not think that the requirements for those derogations to be "necessary" should be interpreted as "strictly necessary". Instead, we request that the ICO adopt a position consistent with that of the EDPB which requires the exporter to evaluate whether a transfer of personal data can be considered necessary (rather than strictly necessary) for the purpose of the particular derogation. It would be unhelpful for the ICO to limit the application of Article 49 UK GDPR beyond the wording of the legislation.

Proposal 5: **Guidance on how to use the IDTA (or other Art 46 transfer tools) in conjunction with the Art 49 Derogations**

Q8: The ICO is considering providing guidance on combining Article 46 transfer tools with Article 49 derogations and welcomes views on this proposal. For example, an exporter has undertaken its transfer risk assessment (TRA), and the IDTA provides appropriate safeguards for some data but not all. In that situation one option is for it to put in place the IDTA for some data and rely on the Art 49 derogations for the rest of the data. [assume same question and analysis when relying on addendum for UK SCCs.]

IRSG response: The IRSG would welcome guidance to this effect which reflects the reality of transfers for many organisations. Given that the legal standard required by Article 46(1) GDPR is vague and open to interpretation, *particularly* when read with the *Schrems II* judgment which requires exporters to carry out highly complicated assessments of third country laws to determine whether they offer equivalent protection to the rights and freedoms of data subjects, we would welcome guidance to permit a waterfall response to the waterfall requirements of Articles 46 and 49. In other words, guidance that encourages exporters to implement Article 46 appropriate safeguards where reasonably practical but also recognises that these may have limitations and *to the extent that* the Article 46 safeguards do not apply for any particular transfer then the exporter would be able to rely on an Article 49 derogation, provided one is available. Allowing exporters to use Article 49 as a backstop in conjunction with an Article 46 appropriate safeguard would also ensure greater protection for data

subjects compared to the alternative of requiring the exporter to pick *either* Article 46 *or* Article 49. There will be certain transfers where Article 46 safeguards are currently not a viable option such as transfers from the UK to the SEC referred to above; for these transfers an Article 49 derogation would be the only option to legitimise the transfer.

Section 2: Transfer risk assessments

Q9: The ICO has produced a draft transfer risk assessment and requests views (provided in free text) on the draft TRA tool including regarding its practicability, the approach to risk and whether it may be used for low risk transfers. The ICO invites suggestions for example transfer scenarios which would be useful to include (Q10).

IRSG response:

We welcome the use of plain English in the TRA which will be useful for SME UK controllers and is a practical document. We note that the TRA is to be used for low risk transfers and would welcome a document which is shorter in length to reflect the risk of the transfer.

Further specific feedback is as follows:

- We welcome the ICO's position that the TRA should not focus on whether third party access is permitted but whether the laws and practices include safeguards which are similar in their objectives to the principles of UK law and whether the possibility of third party access is low regardless of the legal regime. We also welcome the ICO's position that UK controllers can consider the facts of a transfer, the impact on data subjects and any risk of harm (the concept of which is embedded into Article 24 UK GDPR).

- The ICO notes that some jurisdictions should be obviously lower risk, for instance where there is rule of law or robust regulation of third party access to data (although there is no "shortcut" TRA approach for obvious jurisdictions). The IRSG would welcome lists of countries which fall into buckets interpreted by the ICO as high, medium and low risk (in essence a traffic light system).

- For reasons of legal cost it would also be invaluable if the ICO were to provide: (i) country assessments which could be used consistently by all UK controllers, (Step 2 Table A of the TRA) and; (ii) assessments of third party access or surveillance regime (Table D, Step 3), as it is our view that it is untenable to rely on importer's assistance in this regard. Even if they were willing and had the financial means to purchase highly specialised legal advice, the laws and practices of third countries are in many cases esoteric and open to different interpretations. We are already seeing differences in opinions among law firms advising on the same third country laws which is inevitable given the ambiguity in the underlying laws. This adds considerable complexity and cost to the process without delivering any discernible benefits to data subjects. An approved third country comparative assessment and traffic light system cutting through

the complexity of these laws would greatly assist SMEs when determining whether transfers are low / medium / high risk.

- We would welcome clarity on which reports the ICO is referring to when it highlights reports issued by the Foreign Commonwealth and Development Office and charities in the guidance.

- More complex transfer scenarios will require a more forensic analysis and the ICO highlights situations such as multijurisdictional arrangements, novel technology usage, and countries with a questionable human rights record that could produce a high risk and where relying on the ICO's TRA will not be sufficient. We would welcome ICO guidance with regards to what an appropriate assessment would look like in such circumstances and hypothetical worked examples where in the ICO's view a variety of transfers of this nature could continue despite being high risk.

- We welcome that the TRA highlights the importance of focusing on "risk" where an opinion on a jurisdiction is difficult to form. This approach, allied to the pragmatic risk mitigations given, provides practical and considered support which recognises the importance of maintaining data flows while providing proportionate protections consistent with Article 24 of the UK GDPR.

- The guidance as drafted suggests that for high risk transfers, where the TRA is not the suitable tool, controllers should rely instead on an Article 49 UK GDPR derogation. If this is the ICO's position, then we request it be clearly stated.

Section 3: ICO model international data transfer agreements

Proposal 1: New set of standard data protection clauses

Q11: The ICO has requested views on the draft IDTA including responses to specific questions regarding opinions on useability, effectiveness, preference for a modular approach, changes to the mandatory clauses.

Our specific feedback is as follows:

- **Adding parties over time**: More than two parties may enter into the IDTA. We request that the ICO include a mechanism in the final form IDTA where new parties can be added over time, without requiring agreement in writing (clause 5.2) e.g. agreed via notice which is not objected. This would be welcome for organisations reliant on the IDTA for intra-group transfers where new group companies may be created or acquired over time and therefore need adding to the IDTA when they are, or other entities may be closed and require removal.

- **Processor to controller transfers**: As with the new EU SCCs, the ICO has ensured that the IDTA is appropriate for use in C2C, C2P, and P2P scenarios. The IDTA does not, however, contain any clauses to address cross-border transfers from P2C which is included in the new EU SCCs. We

would welcome the inclusion of clauses to cover processor to controller transfers to ensure consistency for organisations with both UK and EU operations. Such clauses would cover transfers made by a UK processor of a non UK GDPR regulated controller to another separate independent controller.

- **Review Dates:** In the tables (p18), for any transfers which are not "one off", the parties are required to select "Review Dates", which will determine the frequency of reviews to ensure that the IDTA continues to provide appropriate safeguards. Each Party is contractually obliged to review the IDTA at the Review Dates. The options for a review are at least once each: month, quarter, 6 months or year. The periods offered will put too much of an administrative burden on organisations which are utilising the IDTA with regards to ongoing review. The period of the review, should be longer (e.g. 3 years) or at the discretion of the parties and the period should not have to be explicitly specified (as with the EU SCCs), provided the IDTA continues to provide appropriate protection.

- **The "if applicable" approach of the IDTA mandatory clauses:** The IDTA is made up of provisions (via caveat drafting) which are designed to be disapplied depending on the nature of the parties (e.g. if the importer's processing is subject to UK data protection law, then the importer does not need to comply with clauses regarding data subject rights (on the basis that they will be directly applicable)). The parties have the ability to amend the IDTA to remove provisions which do not apply. On the basis of the drafting, it seems such provisions will automatically be disapplied meaning in practice there seems to be no benefit from undertaking this exercise. Accordingly, we see limited benefit of including this as an option for controllers (unhelpful hybrid between modular and caveat drafting).

- **Mandatory Clauses**:

    - 8.3.1: IRSG considers that the expectation that the exporter can seek advice from the importer on "local laws" and customs seems to be a conflict of interest with those of the importer who may tell the exporter whatever they want to hear to win the work. This would be an issue in jurisdictions where importers do not have a UK presence, within the enforcement scope of the UK GDPR. The importer is also under a continuing obligation to verify whether local laws change and inform an exporter if such a change would impact its ability to comply with its obligations under the IDTA. "Local Laws" is widely defined which raises issues regarding the quality of knowledge of the importer and their technical ability to comply with these provisions, particularly if they are an MSME.

    - 8.2: the Exporter is under an obligation to provide the Importer with a copy of the completed TRA, upon request. The Importer is bound to a contractual promise that prior to entering into the IDTA that it has provided the exporter with "all relevant information" to enable the importer to undertake the TRA. The position is contractually circular and it is difficult to envisage how an exporter could enforce an obligation to undertake an activity (provision of information for the TRA), which must happen before the IDTA is executed.

- 10/12: - The IDTA provides that both importer and exporter agree to provide the ICO with certain information (including the IDTA, any TRA, and the importer's information regarding local laws) where it reasonably requests it. These provisions place a direct obligation on an importing entity who perhaps might have no other link to the UK, to provide information to a UK-based regulatory information request. It could act as a deterrent to organisations wishing to do business with UK entities. We request that the ICO narrow the scope of this clause to apply to the exporter (as they will have all relevant information) only or to an importer subject to UK GDPR (depending on the final scope).

- 14: The importer (where the UK GDPR does not apply) is obliged to ensure each data subject is provided with details of the Importer, the purposes of the Importer's processing and recipients of transferred data. This information can be provided by the exporter. Given complicated supply chains we consider it highly unlikely that controller exporters will agree to provide transparency information on behalf of individual importers to data subjects (not required pursuant to Art 13/14 UK GDPR). Further, in many circumstances the importer may not have the direct relationship with data subjects to provide this information. In the event of multiple Importers being party to the IDTA, it is difficult to see how this will work in practice without creating confusion for the data subject.

- 19.3: Under the IDTA, the Importer must be able to always easily communicate with Data Subjects in the English language without undue delay. Depending on the counterparty (receiving data in a restricted country), this may not be technically possible to comply with.

- Commercial provisions: the IDTA contains a range of commercial provisions. We wish to agree such provisions as a matter of contract and it seems inappropriate for such positions to be determined by the ICO.

Q12, the ICO will include a number of guidance templates: (i) optional TRA extra protection clauses; (ii) optional commercial clauses; (iii) a template to make changes to the IDTA; (iv) a multi-party IDTA; and (v)an example of a completed TRA & IDTA. The ICO requests identification of any additional guidance templates

IRSG response

N/A

Proposal 2: The adoption of model data transfer agreements issued in other jurisdictions

The ICO is considering issuing an addendum to model data transfer agreements from other jurisdictions. The UK GDPR addendum to the European Commission SCCs (UK SCC Addendum) has been published as an example

- Q13: is this helpful?

- Q14: The ICO invites views on the addendum to the European Commission SCCs.

IRSG response:

We very much welcome this approach, particularly in relation to the most pressing need for certainty and consistency as between the EU and UK approach to standard contractual clauses. The proposed addendum to the European Commission SCCs will allow exporters with operations in both the UK and the EU to have a consistent set of SCCs to address those transfers.

Regarding the addendum to the European Commission SCCs, we request that the ICO considers in consultation with DCMS whether it would be possible to streamline the process further by enacting the operative provisions of the addendum in the proposed revisions to UK data protection laws. Primary legislation could set out powers for the Secretary of State to pass secondary legislation approving and amending where necessary for use in UK law model transfer agreements from third countries. This would considerably reduce the amount of repapering work required for UK transfers easing the regulatory burden for UK exporters yet still preserving the rights and freedoms of data subjects. The same legislation could also be used for other model clauses issued in other jurisdictions where the UK determines that they offer appropriate safeguards.

If legislation is not viable then as a minimum we request that the addendum to the European Commission SCCs (UK SCCs Addendum) be adopted as an approved transfer mechanism under Article 46(2)(c) UK GDPR, as soon as possible (including if it is adopted prior to the IDTA).

Our reading of the UK SCCs Addendum is that it includes administrative amendments to the European Commission Standard Contractual Clauses rather than any substantive obligations with regards to data protection. Please may the ICO include clarification as to when the UK SCCs Addendum and the European Commission Standard Contractual Clauses may be in conflict driving the need for the "hierarchy" clause 7 in the draft addendum. In addition, as drafted, clause 7 of the Addendum could be interpreted to mean that where the *unamended* EU transfer SCC (Clauses) offer a greater protection to data subjects than the Addendum, then the unamended EU transfer SCC Clauses shall prevail. Presumably that is not the intention? Presumably the intention is that for the purposes of Article 46 of the UK GDPR, the Clauses *as amended by the Addendum* will apply; there is therefore no need for a hierarchy clause (at least not between the Addendum and the Clauses).

Proposal 3

The ICO invites views regarding the timing for the disapplication of the existing Directive SCCs. The ICO is proposing that starting from the date 40 days after that IDTA is laid before Parliament (assuming there are no Parliamentary objections to the IDTA), the Directive SCCs would be disapplied: (i) at the end of three months for new Directive SCCs; and (ii) at the end of a further 21 months for all Directive SCCs.

IRSG response

Our view is that a longer transition period should be provided (e.g. a period of 6 months to introduce the IDTA for new arrangements and a further 26 months (i.e. 30 months in total) to repaper existing

arrangements. To the extent, the UK SCCs Addendum does not materialise then the three month period for using the IDTA for new contracts will be ambitious as organisations are likely to need time to amend recently drafted (in light of the new EU SCCs) privacy documentation to include two sets of standard data protection clauses and ensure these fit together appropriately without conflict.