Brussels, October 2021

BSA | The Software Alliance

Submission to the ICO re: Consultation on International Transfers Under UK GDPR

BSA | The Software Alliance ("BSA"),[1] the leading advocate for the global software industry, welcomes the opportunity to provide feedback on the ICO consultation on international transfers under UK GDPR. Our members are business-to-business companies that create the technology products and services that power other companies, including cloud storage services, customer relationship management software, identity management services, and workplace collaboration software. These technologies must transfer data across international borders – and across legal systems – to provide the global products and services that customers demand. As a result, supporting the trusted and responsible transfer of data across borders is a core issue for BSA members.

We commend the ICO for recognizing the importance of international data flows and for prioritizing high standards of data protection, trust, and confidence.

Our comments focus on four aspects of the consultation:

1. ***Strongly Supporting the Creation of Addendums for Data Transfers***. The consultation includes a draft international data transfer agreement ("IDTA") in the form of an addendum to the European Commission's Standard Contractual Clauses ("EU SCCs"). We strongly support this work and encourage the ICO to both finalize this draft addendum and to create additional template addendums for additional jurisdictions in the future. Such addendums help companies implement the UK's data transfer obligations in a practical way because they are expressly designed to interoperate with other data protection laws.

2. ***Ensuring Consistency in Revisions to Guidance on International Transfers***. The consultation also proposes new guidance on international transfers. In addressing the extraterritorial reach of UK GDPR, we encourage the ICO to recognize that whether a processor outside the UK is subject to UK law should depend on the relevant circumstances. We also support a flexible approach to guidance addressing the types of transfers deemed "restricted" under UK law.

[1] *BSA's members include: Adobe, Akamai, Atlassian, Autodesk, Bentley Systems, BlackBerry, Box, Cloudflare, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, and Zoom.*

3. ***Promoting Voluntary Risk Assessment Tools***. We welcome the ICO's efforts to help companies assess the risks associated with international transfers, including through the draft transfer risk assessment tool, which the consultation makes clear is only one way – and not the only way – for companies to conduct risk assessments. We encourage the ICO to consider adopting a high-level summary of this tool, since the detailed nature of the tool may provide more information than suitable for some organizations, particularly small and medium enterprises for which the assessment may be more straightforward. In addition, we encourage the ICO to ensure the tool recognizes the appropriateness of assessing a set of transfers, such as conducting an assessment prior to commercializing or using a service that transfers the same types of data for the same purposes at scale.

4. ***Allowing Sufficient Transition Time***. The consultation also addresses the timeline for transitioning away from UK recognition of the EU SCCs, after a final IDTA is issued. We encourage the ICO to consider basing this timeline not only on when the new IDTA is laid before Parliament, but also when the final IDTA addendum to the EU SCCs is ready for adoption by companies – given that many organizations will want to utilize such an addendum. We also encourage extending the initial transition time to six months, from three months.

I. Supporting the Creation of Template Addendums for Data Transfers (Qs 13, 14)

BSA strongly supports the ICO's work to develop an IDTA in the form of an addendum to model data transfer agreements from other jurisdictions. We particularly welcome the example EU addendum included in the consultation, which would allow companies to amend the EU SCCs to work in the context of UK data transfers.

We encourage the ICO to continue this work, including to: (1) finalize the example addendum to the EU SCCs, so that companies may implement the IDTA by adopting this addendum, and (2) issue similar addendums to model transfer agreements in other countries, including in the future as other countries adopt such model transfer agreements. In these efforts, we encourage the ICO to focus on the creation of template addendums, which companies tailor and implement based on the actual transfers they are undertaking. This approach will provide companies with clear guidance on the appropriate substantive provisions for safeguarding data that are to be included in an addendum, without requiring companies to conform to the same strict format of document.

The approach of issuing IDTA in the form of an addendum is helpful because:

- *It is interoperable.* Companies that provide services in more than one country must identify – and implement – the additional privacy and data protection requirements imposed by another country's legal framework. Template addendums help companies do this efficiently, by listing those additional requirements which can then be mapped to existing legal obligations. This approach embodies the interoperable model companies strive for, while ensuring that organizations can readily identify and adopt measures to comply with each country's standards of data protection and privacy.

- *It is economically valuable*. Issuing an IDTA as an addendum is also economically valuable. This approach decreases cost of doing business in the UK, since it helps companies leverage the compliance work they have done for another country to comply with UK requirements. As a result, it may encourage more companies to enter the UK market than if those companies had to undertake standalone compliance efforts and enter into a standalone IDTA for each set of transfers.

- *It promotes global harmonization*. By recognizing the benefits of issuing model addendums, the ICO can establish a model that encourages data protection authorities in other countries to similarly issue addendums in support of international transfers, further supporting this interoperable approach to data transfers. Globally, several other regulators are considering adopting model contract clauses for cross-border transfers. The ICO's efforts can become a model for other regulators and help to ensure model clauses can work together in practice to promote high data protection standards.

In addition to finalizing the addendum for the EU SCCs, we encourage the ICO to issue addendums for countries that have finalized their own model transfer agreements, such as New Zealand. We also encourage the ICO to closely monitor the creation of model transfer agreements in other countries that may be implementing a new national data protection law, such as Brazil, and to issue new UK addendums as such other model agreements are finalized.

The consultation also asks specifically for views on the addendum to the EU SCCs. As noted above, we strongly support finalizing this addendum, so that companies may rely on the addendum to comply with the IDTA's requirements.

II. Guidance on International Transfers

BSA also encourages the ICO to adopt revisions to its guidance on international transfers that ensure UK law is applied consistently. We set out below our views on both the proposed revisions to guidance on the interpretation of the extraterritorial effects of Article 3 UK GDPR and on proposed revisions to the interpretation of Chapter V UK GDPR.

A. Guidance on Interpretation of Extraterritorial Effects of Article 3 UK GDPR (Qs 1-2)

Proposals 1 and 2 address the application of UK law to processors located outside the UK.

This is a key issue for BSA members, because as enterprise software companies, BSA members generally act as data processors by providing technologies and services used by other businesses that decide how to collect and process personal data. For example, our members may store data in the cloud on behalf of other companies or provide software-as-a-service tools that other companies can customize to suit their needs. Because their role is to process data on behalf of those other companies, processors often lack visibility into the data run through such tools and services.[2]

[2] In certain circumstances, however, BSA members may also act as controllers. For instance, a company that operates principally as a data processor may nonetheless be treated as a controller when it collects data for the purposes of providing services directly to consumers.

For Proposals 1 and 2, we encourage the ICO to ensure its guidance treats these situations similarly – and reflects that whether the processor is subject to UK law in either scenario depends on the circumstances.

- ***Proposal 1*** *involves the processing by a non-UK processor for a UK-based controller (i.e., an Article 3(1) controller).* The question is whether processing by a UK-based controller's non-UK processor is always governed by UK GDPR. We agree with the ICO's stated view: that whether the non-UK processor is subject to UK law should depend on the circumstances.

  In many cases, data processors will serve hundreds or thousands of controllers, only some of which may be subject to UK law. UK law should extend to non-UK processors only in the context of processing done on behalf of a UK-based controller. If the opposite conclusion were reached – and non-UK processors were always subject to UK law, regardless of whether the processing at issue was performed on behalf of a UK-based controller – it could lead to wide-ranging application of UK law and create inadvertent conflicts with other laws. For example, a processor could handle data on behalf of three companies: one based in the UK, one in Canada, and one in New Zealand. In that scenario, UK law should only extend to the processing undertaken on behalf of the UK controller; extending it further could inadvertently create conflicts with Canadian law or New Zealand law.

  The extension of UK law to non-UK processors should instead depend on the relevant circumstances, and specifically on whether the processing at issue is done on behalf of the UK-based controller. In many cases, this may be readily reflected in a data processing agreement that incorporates Article 28's requirements and states the relevance of UK law, ensuring that companies clearly identify the operative law in that agreement. We accordingly urge the ICO to adopt Option 2, which recognizes that whether the processor is also covered by Article 3(1) will always depend on the circumstances. We also encourage the ICO to recognize that the most relevant circumstance is whether the processing at issue is done on behalf of the UK-based controller.

- ***Proposal 2*** *involves the processing by a non-UK processor for a non-UK controller, where the controller is subject to UK law because its processing involves either offering goods or services to people located in the UK or relates to monitoring the behavior of people in the UK (i.e., an Article 3(2) controller).* The question is whether processing by the non-UK processor is always governed by UK GDPR. We urge the ICO to treat this scenario as analogous to the scenario above, and to recognize that application of UK law to the non-UK processor depends on the circumstances.

  The consultation notes that the ICO is inclined to take the opposite view – i.e., that such processors are *always* subject to UK law. However, it bases that conclusion on the recognition that when a non-UK processor is carrying out processing relating to the controller's targeting or monitoring activity, it should be subject to UK law. We agree with that statement – but believe that determining whether a processor is in fact carrying out activities relating to the controller's targeting or monitoring activity necessarily requires an analysis of the relevant circumstances, particularly whether the specific processing at issue relates to customers in the UK.

For example, a non-UK processor may provide cloud storage services to a non-UK controller – but the controller may use those services to store information about customers in the UK, Canada, and New Zealand. The non-UK processor should accordingly be subject to UK law only for processing related to customers located in the UK – but identifying that segment of the processing activities requires an analysis of the relevant circumstances. Again, those circumstances are likely to be reflected in a data processing agreement that incorporates Article 28's requirements and states the relevance of UK law.

We accordingly urge the ICO to adopt Option 2, which recognizes that whether the processor is also covered by Article 3(2) will always depend on the circumstances. We further encourage the ICO to recognize that the most relevant circumstance is whether the specific processing at issue relates to customers in the UK.

B. Guidance on Interpretation of Chapter V UK GDPR (Qs 4, 6, 7)

Proposals 1 and 3 address important questions about the scope of "restricted transfers" under the UK GDPR. Proposal 4 addresses circumstances under which derogations may be appropriate

- *Proposal 1 suggests that the ICO revise its guidance to state there is no "restricted transfer" when data flows within a legal entity*. As a result, when a corporate entity transfers data within the same legal entity, it would have to comply with general UK GDPR obligations but not the transfer requirements set out Chapter V. We appreciate the flexibility in the ICO's proposed approach and see both benefits and potential drawbacks to this change. In determining whether to adopt this change, we encourage the ICO to consider the scope of companies that would benefit from this approach given their processing operations footprints and tools currently used for intra-company transfers, the different types of relationships and levels of control exercised between corporate entities, and the overarching need for any change to ensure the data at issue would remain appropriately protected and in line with the UK's high data protection standards.

- *Proposal 3 addresses whether transfers by companies subject to UK law to companies located outside the UK are always "restricted."* Under current ICO guidance, such transfers would not be restricted – and thus would not need to comply with transfer requirements set out in Chapter V – when the receiving entity is itself subject to the UK GDPR. The ICO proposes changing this guidance, to treat a transfer as restricted so long as the receiving entity is located outside the UK – even if that company is subject to UK GDPR. We can identify few benefits to this approach, because a receiving entity subject to UK law will necessarily need to comply with UK legal requirements. We encourage the ICO to adopt Option 1, which would maintain the current guidance.

- *Proposal 4 addresses whether guidance concerning derogations should be updated.* The ICO suggests updating this guidance in line with how UK courts may interpret it as well as guidance set out in relevant UK GDPR recitals. We believe that any requirement for a derogation should be assessed on the basis of it being "necessary" as opposed to solely being "strictly necessary." The derogations in Article 49 inherently carve out very specific conditions to be met when an organization wants to rely on such a derogation. For example, the threshold for using consent as

a valid basis for international transfer is higher and conditions to be met more specific than required for using consent as a legal basis for processing for other requirements of the UK GDPR. The proposed approach would therefore help to ensure that on the rare occasions when a derogation may be needed, it can be obtained in the most efficient manner possible.

III. **Tools for Assessing Risk** (Q9)

We support the ICO's efforts to help companies assess the risks associated with international transfers, and its focus on providing voluntary and practical tools.

The draft transfer risk assessment ("TRA") tool contains a large amount of information that may be helpful to companies in assessing the potential risks associated with their transfers. Critically, the TRA tool recognizes that it is one approach for conducting a transfer risk assessment – and that there are other ways for companies to carry out these assessments. We also appreciate the TRA tool's recognition that conducting such assessments can be a "complicated exercise" for organizations, particularly those with limited resources, and its focus on the key issues of enforcing an IDTA and assessing the legal framework of the destination country.

In our view, two aspects of the TRA tool are particularly helpful:

- Its focus on helping companies identify the relevant parts of a destination country's legal framework. The TRA tool acknowledges that in assessing the potential risk of third-party access to data, companies need not look at the "whole regime" of a destination country, but instead "only those parts . . . which are relevant to your restricted transfer" helps companies focus their resources on the most relevant parts of the transfer assessment.[3] Similarly, the guidance emphasizes that a company's assessment should focus "not whether third party access, including surveillance, is permitted by local law, but rather whether the laws and practices include safeguards which are sufficiently similar in their objectives to the principles which underpin UK laws."[4]

- Its focus on the range of additional safeguards that companies can adopt to address potential risks. In particular, Table G identifies types and levels of measures that may supplement IDTA safeguards. We commend the ICO for identifying in this table a range of safeguards that reflect organizational and contractual measures, in addition to technical measures companies could adopt, and for recognizing that different levels of such measures may be appropriate in different circumstances, depending on the relevant transfer. We urge the ICO to continue updating Table G over time to expand the identified measures.

At the same time, we appreciate that the detailed nature of the TRA tool may also make it more burdensome for some companies to readily use the tool, particularly those without large compliance teams. For that reason, we encourage the ICO to consider issuing an executive summary of the TRA tool, which may create a practical way for companies of all sizes to easily identify the foundational questions involved in a TRA assessment. This sort of user-friendly executive summary could also cross-reference

[3] TRA Tool, Page 5.
[4] TRA Tool, Page 4.

the full TRA, so that companies that want further details on one aspect could more easily interact with the larger amount of detail in the full TRA tool.

Finally, we encourage revisions that more expressly recognize that assessments may be performed for a set of transfers, such as the set of transfers involved in providing a particular product or service. Specifically, we encourage adding language to the introductory sections of the TRA tool that expressly recognizes the appropriateness of conducting a risk assessment prior to commercializing or using a service that transfers the same types of data for the same purposes at scale.

IV. Allowing Sufficient Transition Time for Discontinuing Use of EU SCCs (Q15)

The consultation also addresses the transition away from UK recognition of the EU SCCs, after issuance of the final IDTA.

Section 3, Proposal 3 suggests a timeline for that transition based on when the new IDTA is adopted, with the transition starting 40 days after the IDTA is laid before Parliament. After that time, the EU SCCs would be disapplied: (1) after three months for new SCCs, and (2) after an additional 21 months for existing SCCs.

We recommend two changes to this timeline:

- First, the timeline should be based on when the final IDTA template addendum to the EU SCCs is ready for adoption by companies, rather than only on when the new IDTA is laid before Parliament. This would ensure that companies currently relying on the EU SCCs can transition to the addendum version of the IDTA. As we noted at the outset, our companies find significant practical and economic value in implementing the IDTA through such an addendum – and the transition time should permit companies to transition from reliance on the EU SCCs to reliance on the IDTA addendum to the EU SCCs, without requiring them to first adopt the full standalone IDTA while the addendum is finalized.

- Second, and particularly if the IDTA addendum to the EU SCCs is not finalized at the same time as the IDTA, the timeline for disapplying EU SCCs to new contracts should be extended to six months, rather than three months. This would permit companies additional time to implement compliance practices aligned with the new IDTA.

We would welcome the opportunity to engage further with the ICO on these issues.

For further information, please contact:

Thomas Boué, Director General, Policy – EMEA
thomasb@bsa.org or +32.2.274.1315

ICO consultation

International transfers under UK GDPR

Date

Information Commissioner's Office

Contents

Now the UK has left the EU and following the CJEU Schrems II decision last year, it is the right moment for the ICO to update our guidance and transfer tools about international transfers.

The ICO recognises the importance of international data flows to the UK's digital economy. We aim to enable a system that maintains high standards of data protection, and trust and confidence. This system should also be a proportionate and risk-based implementation of UK GDPR. This also forms part of a wider UK package to support international transfers. This includes the Government's approach to adequacy assessments of third countries, which the ICO will support with independent advice.

We are consulting on these questions and associated products to provide greater regulatory certainty and to assist organisations to comply with the law. The consultation will also enable us to understand the practical impacts of the proposed approaches below. The ICO is planning the following in 2021:

- update our guidance on Chapter V UK GDPR and restricted transfers;
- provide guidance on how to conduct an international transfers risk assessment; and
- issue an ICO IDTA (international data transfer agreement - the ICO version of SCCs under the UK GDPR).

This consultation is split into three sections:

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

Section 2: Transfer risk assessments

Section 3: ICO model international data transfer agreements

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

A. Interpretation of the extra-territorial effects of Article 3 UK GDPR

Article 3 UK GDPR:

> [1] This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the United Kingdom, regardless of whether the processing takes place in the United Kingdom or not.
>
> [2] This Regulation applies to the relevant processing of personal data of data subjects who are in the United Kingdom by a controller or processor not established in the United Kingdom where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the United Kingdom; or
>
> (b) the monitoring of their behaviour as far as their behaviour takes place within the United Kingdom.
>
> [2A] In paragraph 2, "relevant processing of personal data" means processing to which this Regulation applies, other than processing described in Article 2(1)(a) or (b) or (1A).
>
> [3] This Regulation applies to the processing of personal data by a controller not established in the United Kingdom, but in a place where domestic law applies by virtue of public international law.

The interpretation of the extra-territorial effects of Article 3 UK GDPR is relevant to both:

- the interpretation of a “restricted transfer”; and
- consideration of what appropriate safeguards are needed (if any) under Chapter V UK GDPR.

It is broadly settled when UK GDPR applies to a controller or processor outside of the UK under Art 3.1 and 3.2. For further information, read our guidance on the definition of controllers and processors.

There are two key points where it may be helpful for the ICO to provide guidance. That is, whether or not UK GDPR inevitably governs processing by:

- (i) an overseas processor of a "UK GDPR controller" (a controller whose processing falls within the scope of UK GDPR); and
- (ii) an overseas joint controller with a UK joint controller.

Background

First, we start with a UK controller whose processing activities fall within the scope of Art 3(1) (a UK-based controller). Our consultation asks whether processing by a UK-based controller's overseas processor or overseas joint controller is **inevitably** governed by UK GDPR. This turns on whether processing by such overseas processor or overseas joint controller, is inevitably carried out in the context of the activities of the UK-based controller's UK establishment.

The circumstances in which activities will be carried out in the context of a UK establishment's activities are wide-ranging. It is possible for an overseas company to process data in the context of the establishment of an entirely separate company.

A simplified example, following the reasoning in the Google Spain judgment: a US search engine has a UK subsidiary which helps it to market advertising to UK users of the US search engine. The US search engine may be processing in the context of the UK subsidiary's UK offices, even though the UK subsidiary is not involved in the actual operation of the search engine.

The role of a processor is set out in Art 4(8) and Art 28. Our consultation asks whether the scope of this role means all overseas processors with a UK-based controller, are processing in the context of the activities of that controller's UK establishment. Or, if that was the intention, would the language of UK GDPR have been explicit?

Second, we start with an overseas controller whose processing activities fall within the scope of Art 3(2) (an Art 3(2) controller). Its processing must either relate to the offering of goods or services to people located in the UK or relate to monitoring the behaviour of people in the UK.

Our consultation asks whether processing by that Art 3(2) controller's overseas processors is inevitably governed by UK GDPR. This question turns on whether the processor's processing activities **inevitably** also **relate to** offering of goods or services to people located in the UK or to monitoring people located in the UK, even though it is the controller's ultimate decision. Or, if that was the intention, would the language of UK GDPR have been explicit?

Finally, we start with a joint controller processing personal data in the context of its UK establishment (within the scope of Art 3(1)), with an overseas joint controller.

Our consultation asks whether that overseas joint controller is inevitably processing in the context of its UK joint controller's establishment. Or, would it depend on the specific circumstances?

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

Option 1: The processor is always covered by UK GDPR Art 3(1).

Its processing activities have been authorised by a controller whose processing is covered by Art 3(1) of 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.

Things to consider:

- This interpretation is easy to understand and apply.
- How Google Spain applies to UK GDPR, and does this interpretation align with its reasoning?
- It protects both UK controllers and UK data subjects when their data is being processed outside the UK.
- It maintains a level playing field for UK processors who are competing with non-UK processors for contracts.
- These processors already have to comply with a contract governed by Art 28 (directly or indirectly if a sub-processor) which contains most of the UK GDPR obligations.
- If this interpretation is most likely to be followed by the UK courts, it prepares processors and sub-processors of UK GDPR controllers for the potential risk of ICO oversight and claims by data subjects for breach of UK GDPR processor obligations.
- Is it appropriate for the ICO to have oversight of these overseas processors and sub-processors?
- Should data subjects be able to bring claims for breach of UK GDPR obligations against these overseas processors and sub-processors?

Option 2: Whether the processor is also covered by Art 3(1) will always depend on the circumstances.

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.

Things to consider:

- This interpretation follows the language of UK GDPR.

- If the intention was the increased level of extra-territorial reach in Option 1, would this require express language in UK GDPR?
- Is the extra-territoriality of UK GDPR sufficiently covered by Art 3(2) UK GDPR?
- This interpretation is more consistent with the approach of EDPB in relation to the EU GDPR.
- Are UK controllers and UK data subjects whose data is processed by overseas processors and sub-processors sufficiently protected by Art 28 contract and the international transfer rules in Chapter V?
- This option may be more complex to apply; it will require an assessment whether Art 3(1) or (2) applies to an overseas processor or sub-processor.

Q1. As set out above, there are valid points in favour of both options. Our current preference is for Option 2. The key reason being that such extra territoriality should have explicit language in UK GDPR, but we can also see the logic of Option 1 which flows from the reasoning in Google Spain.

The ICO would welcome evidence on the implications of both options. Please identify any relevant privacy rights, legal, economic or policy considerations and implications.

☐ **Option 1**

☒ **Option 2**

BSA | The Software Alliance ("BSA"),[1] the leading advocate for the global software industry, welcomes the opportunity to provide feedback on the ICO consultation on international transfers under UK GDPR. Our members are business-to-business companies that create the technology products and services that power other companies, including cloud storage services, customer relationship management software, identity management services, and workplace collaboration software. These technologies must transfer data across international borders – and across legal systems – to provide the global products and services that customers demand. As a result, supporting the trusted and responsible transfer of data across borders is a core issue for BSA members

BSA encourages the ICO to adopt revisions to its guidance on international transfers that ensure UK law is applied consistently.

The application of UK law to processors located outside the UK is a key issue

[1] *BSA's members include: Adobe, Akamai, Atlassian, Autodesk, Bentley Systems, BlackBerry, Box, Cloudflare, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, and Zoom.*

for BSA members, because as enterprise software companies, BSA members generally act as data processors by providing technologies and services used by other businesses that decide how to collect and process personal data. For example, our members may store data in the cloud on behalf of other companies or provide software-as-a-service tools that other companies can customize to suit their needs. Because their role is to process data on behalf of those other companies, processors often lack visibility into the data run through such tools and services.[2]

For Proposals 1 and 2, we encourage the ICO to ensure its guidance treats these situations similarly – and reflects that whether the processor is subject to UK law in either scenario depends on the circumstances.

- ***Proposal 1*** *involves the processing by a non-UK processor for a UK-based controller (i.e., an Article 3(1) controller).* The question is whether processing by a UK-based controller's non-UK processor is always governed by UK GDPR. We agree with the ICO's stated view: that whether the non-UK processor is subject to UK law should depend on the circumstances.

  In many cases, data processors will serve hundreds or thousands of controllers, only some of which may be subject to UK law. UK law should extend to non-UK processors only in the context of processing done on behalf of a UK-based controller. If the opposite conclusion were reached – and non-UK processors were always subject to UK law, regardless of whether the processing at issue was performed on behalf of a UK-based controller – it could lead to wide-ranging application of UK law and create inadvertent conflicts with other laws. For example, a processor could handle data on behalf of three companies: one based in the UK, one in Canada, and one in New Zealand. In that scenario, UK law should only extend to the processing undertaken on behalf of the UK controller; extending it further could inadvertently create conflicts with Canadian law or New Zealand law.

  The extension of UK law to non-UK processors should instead depend on the relevant circumstances, and specifically on whether the processing at issue is done on behalf of the UK-based controller. In many cases, this may be readily reflected in a data processing agreement that incorporates Article 28's requirements and states the relevance of UK law, ensuring that companies clearly identify the operative law in that agreement. We accordingly urge the ICO to adopt Option 2, which

[2] In certain circumstances, however, BSA members may also act as controllers. For instance, a company that operates principally as a data processor may nonetheless be treated as a controller when it collects data for the purposes of providing services directly to consumers.

recognizes that whether the processor is also covered by Article 3(1) will always depend on the circumstances. We also encourage the ICO to recognize that the most relevant circumstance is whether the processing at issue is done on behalf of the UK-based controller.

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

Option 1: The processor is always covered by 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 Art 3(2). This is because it is carrying out processing relating to the controller's targeting or monitoring activity.

Option 2: Whether the processor is also covered by Art 3(2) will always depend on the circumstances.

The processor's processing activities will not always **relate to** the controller's targeting or monitoring activity.

Things to consider:

- If the intention was that Art 3(2) would always apply to a processor if Art 3(2) applied to its controller, would this need explicit language in UK GDPR?
- If an Art 3(2) controller is sub-contracting its processing which "relates to" targeting and monitoring people in the UK, it is hard to see how that sub-processing does not also relate to such targeting and monitoring.

Q2. The ICO's current intention is to follow Option 1 but there are valid points in favour of both options.

The ICO would welcome evidence on the implications of both options. Please identify any relevant privacy rights, legal, economic or policy considerations and implications.

☐ **Option 1**

☒ **Option 2**

BSA encourages the ICO to adopt revisions to its guidance on international transfers that ensure UK law is applied consistently.

The application of UK law to processors located outside the UK is a key issue for BSA members, because as enterprise software companies, BSA members generally act as data processors by providing technologies and services used

by other businesses that decide how to collect and process personal data. For example, our members may store data in the cloud on behalf of other companies or provide software-as-a-service tools that other companies can customize to suit their needs. Because their role is to process data on behalf of those other companies, processors often lack visibility into the data run through such tools and services.

For Proposals 1 and 2, we encourage the ICO to ensure its guidance treats these situations similarly – and reflects that whether the processor is subject to UK law in either scenario depends on the circumstances.

- ***Proposal 2*** *involves the processing by a non-UK processor for a non-UK controller, where the controller is subject to UK law because its processing involves either offering goods or services to people located in the UK or relates to monitoring the behavior of people in the UK (i.e., an Article 3(2) controller).* The question is whether processing by the non-UK processor is always governed by UK GDPR. We urge the ICO to treat this scenario as analogous to the scenario above, and to recognize that application of UK law to the non-UK processor depends on the circumstances.

  The consultation notes that the ICO is inclined to take the opposite view – i.e., that such processors are *always* subject to UK law. However, it bases that conclusion on the recognition that when a non-UK processor is carrying out processing relating to the controller's targeting or monitoring activity, it should be subject to UK law. We agree with that statement – but believe that determining whether a processor is in fact carrying out activities relating to the controller's targeting or monitoring activity necessarily requires an analysis of the relevant circumstances, particularly whether the specific processing at issue relates to customers in the UK.

  For example, a non-UK processor may provide cloud storage services to a non-UK controller – but the controller may use those services to store information about customers in the UK, Canada, and New Zealand. The non-UK processor should accordingly be subject to UK law only for processing related to customers located in the UK – but identifying that segment of the processing activities requires an analysis of the relevant circumstances. Again, those circumstances are likely to be reflected in a data processing agreement that incorporates Article 28's requirements and states the relevance of UK law.

  We accordingly urge the ICO to adopt Option 2, which recognizes that whether the processor is also covered by Article 3(2) will always depend on the circumstances. We further encourage the ICO to recognize that

the most relevant circumstance is whether the specific processing at issue relates to customers in the UK.

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

Option 1: The overseas joint controller is always covered by UK GDPR Art 3(1).

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 will inevitably be in the context of the UK GDPR controller's UK establishment.

Option 2: Whether the joint controller is covered by UK GDPR Art 3(1) 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.

Things to consider:

- If the intention was that UK GDPR would always apply to an overseas joint controller with a UK joint controller, would this need explicit language in UK GDPR?
- Does the fact that to be a joint controller you must be jointly deciding the purpose and means of processing activities, also mean the overseas joint controller must be processing in the context of its UK joint controller's UK establishment?
- Case law on joint controllers has set a low threshold as to the involvement of a joint controller in decision-making and processing. For an example, see the Facebook Fan page judgment. Does this mean that it is not inevitable for that (minimal) decision-making or processing as joint controllers to always be in the context of the UK joint controller's UK establishment?
- Joint controllership can arise in relation to complex business and other relationships. Do you have examples of joint controller relationships where the overseas joint controller is not processing in the context of the UK controller's establishment?

Q3. The ICO's current intention is to follow Option 2 but there are valid points in favour of both options.

The ICO would welcome evidence on the implications of both options. Please identify any relevant privacy rights, legal, economic or policy considerations and implications.

☐ **Option 1**

☐ **Option 2**

B. Interpretation of Chapter V UK GDPR

Article 44 UK GDPR:

> " Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined".

A transfer falling within Article 44 UK GDPR is referred to as a "restricted transfer". This is because a transfer of personal data to a third country can only take place when the conditions in Chapter V UK GDPR are complied with.

Proposal 1: In order for a restricted transfer to take place, there must be a transfer from one legal entity to another.

This means that it is not a restricted transfer where the data flows within a legal entity. For example, it is not a restricted transfer where an employee takes a laptop outside the UK, or a UK company shares data with its overseas branch.

This reflects the language of Art 44 and the appropriate safeguards in Art 46.

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.

Q4. Please provide us with your views on this proposal. Please highlight any relevant privacy rights, legal, economic or policy considerations and implications.

Proposal 1 suggests that the ICO revise its guidance to state there is no "restricted transfer" when data flows within a legal entity. As a result, when a corporate entity transfers data within the same legal entity, it would have to comply with general UK GDPR obligations but not the transfer requirements set out Chapter V. We appreciate the flexibility in the ICO's proposed approach and see both benefits and potential drawbacks to this change. In determining whether to adopt this change, we encourage the ICO to consider the scope of companies that would benefit from this approach given their processing operations footprints and tools currently used for intra-company transfers, the different types of relationships and levels of control exercised between corporate entities, and the overarching need for any change to ensure the data at issue would remain appropriately protected and in line with the UK's high data protection standards.

Proposal 2: A UK GDPR processor with a non-UK GDPR controller, will only make a restricted transfer to its own overseas sub-processors.

There is only a restricted transfer when the underlying decision to make the transfer is governed by UK GDPR, in particular under Article 5 "Principles relating to processing of personal data", or Article 6 "Lawfulness of processing", or Article 28(2) "Processor".

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).

Q5. Please provide us with your views on this proposal. Please highlight any relevant privacy rights, legal, economic or policy considerations and implications.

Proposal 3: Whether processing by the importer must not be governed by UK GDPR.

Option 1: The ICO maintains our 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. For example, the exporter will not need to carry out a Schrems II risk assessment nor put in place an Art 46 transfer tool.

The exporter and the importer will each need to consider the risks posed to data subjects as a result of overseas laws conflicting with their UK GDPR obligations, in particular Art 5 "Principles relating to processing of personal data".

The ICO will have oversight of the importer's processing under UK GDPR and data subjects will have UK GDPR rights. We acknowledge there may be difficulties in enforcing those rights overseas.

This option assumes that the Chapter V requirements apply only where personal data requires additional protection as it is to be processed other than in accordance with the UK GDPR.

Option 2: The ICO updates our guidance.

Alternatively, the ICO could update our current guidance to reflect that:

- a restricted transfer takes place whenever the exporter is subject to UK GDPR (and may be located in the UK or overseas); 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. If an IDTA is used, it will provide contractual protections for exporters and data subjects seeking to enforce rights against the importer, and more certainty in how to comply with UK GDPR for the exporter and the importer.

We also propose that a restricted transfer would take place when the UK GDPR controller or processor **authorises** an overseas legal entity to process the data (rather than restricted transfers following the data flow). This would allow the restricted transfer to follow the usual contractual relationships while still maintaining the right level of protection for data subject rights.

For example:

- UK Company A authorises UK service provider B to process its personal data.
- UK service provider B uses an overseas sub-processor C.
- Data flows directly from UK Company A to the overseas sub-processor C.
- The restricted transfer is between UK service provider B and overseas sub-processor C, as UK service provider B is **authorising** an overseas separate legal entity to process data.

We are using "authorise" in its widest sense, so it covers both data sharing arrangements and controller-processor contracts.

We also propose that it would not be a restricted transfer when data flows from a UK GDPR processor to its non-UK GDPR controller. This is because the UK GDPR processor cannot be **authorising** (even in its widest sense) its controller to process the data.

Example:

- Overseas non-GDPR Company A appoints UK service provider B as its processor.
- UK service provider B sends the data to its controller, non-GDPR Company A.
- This is not a restricted transfer as UK service provider B cannot be said to be authorising its controller to receive this data, even in the widest sense of that word.

Q6. The ICO's current intention is to follow Option 2 but there are valid points in favour of both options.

The ICO would welcome evidence on the implications of both options. Please identify any relevant privacy rights, legal, economic or policy considerations and implications.

☒ **Option 1**

☐ **Option 2**

Proposal 3 addresses whether transfers by companies subject to UK law to companies located outside the UK are always "restricted." Under current ICO guidance, such transfers would not be restricted – and thus would not need to comply with transfer requirements set out in Chapter V – when the receiving entity is itself subject to the UK GDPR. The ICO proposes changing this guidance, to treat a transfer as restricted so long as the receiving entity is located outside the UK – even if that company is subject to UK GDPR. We can identify few benefits to this approach, because a receiving entity subject to UK law will necessarily need to comply with UK legal requirements. We encourage the ICO to adopt Option 1, which would maintain the current guidance.

Proposal 4: Art 49 Derogations

Article 49:

1. In the absence of adequacy regulations under section 17A of the 2018 Act, or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

    1. In the absence of adequacy regulations under section 17A of the 2018 Act, or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

        (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

        (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

        (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

        (d) the transfer is necessary for important reasons of public interest;

        (e) the transfer is necessary for the establishment, exercise or defence of legal claims;

        (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

        (g) the transfer is made from a register which according to domestic law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by domestic law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46,

including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the Commissioner of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14,inform the data subject of the transfer and of the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point(d) of the first subparagraph of paragraph 1 must be public interest that is recognised in domestic law (whether in regulations under section 18(1) of the 2018 Act or otherwise).

[5A. This Article and Article 46 are subject to restrictions in regulations under section 18(2) of the 2018 Act.]

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

We are considering updating our guidance in line with how UK courts will interpret these provisions and in light of the guidance set out in UK GDPR Recitals 111 to 115. This guidance will be relevant for how we interpret whether a derogation is “necessary and proportionate”.

Q7. Please provide your views on the current ICO guidance about derogations, in particular:

- Should exporters first try to put an appropriate safeguard in place before relying on a derogation?
- Should the requirements for those derogations to be “necessary” be interpreted as “strictly necessary”.
- To what extent may the derogations be relied on for repetitive transfers, regular and predictable transfers and systematic transfers?

Proposal 4 addresses whether guidance concerning derogations should be updated. The ICO suggests updating this guidance in line with how UK courts may interpret it as well as guidance set out in relevant UK GDPR recitals. We believe that any requirement for a derogation should be assessed on the basis of it being "necessary” as opposed to solely being “strictly necessary.” The derogations in Article 49 inherently carve out very specific conditions to be met when an organization wants to rely on such a derogation. For example, the threshold for using consent as a valid basis for international transfer is higher and conditions to be met more specific than required for using consent as a legal basis for processing for other requirements of the UK GDPR. The proposed approach would therefore help to ensure that on the rare occasions when a derogation may be needed, it can be obtained in the most efficient manner possible.

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

We are considering providing guidance on how to combine IDTAs (and other Art 46 transfer tools) with the Art 49 Derogations.

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.

Having the IDTA in place for **all the data**, may make it easier to meet the requirements of the Art 49 derogations. For example, explicit consent may only need to cover those risks which do not have appropriate safeguards under the IDTA. Or for the other Art 49 derogations it may make it easier to rely on the restricted transfer of that data being “necessary and proportionate”, given that there are some protections in place.

Q8. Please provide us with your views on this proposal. Please highlight any relevant economic or policy considerations and implications.

Section 2: Transfer risk assessments

Proposal 1: A transfer risk assessment tool.

The Schrems II judgment is an EU case which is retained in UK law by the EU Withdrawal Act. It is therefore important the ICO provides guidance about how this judgment applies to the application of UK GDPR. The judgment found that:

- SCCs, providing appropriate safeguards for restricted transfers under Article 46(2)(c), must provide a level of protection "essentially equivalent" to that guaranteed within the European Union by the GDPR, read in the light of the Charter of Fundamental Rights of the European Union, and
- an assessment of the level of protection provided by an SCC in the destination country, must be performed before making a restricted transfer of data.

The ICO has produced a **draft** transfer risk assessment tool (TRA tool) to assist when completing the risk assessment required following the decision in Schrems II. This TRA tool (Annex 1) is only one method for carrying out a risk assessment and it is for routine transfers only. You are free to use other methods to carry out 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?

We support the ICO's efforts to help companies assess the risks associated with international transfers, and its focus on providing voluntary and practical tools.

The draft transfer risk assessment ("TRA") tool contains a large amount of information that may be helpful to companies in assessing the potential risks associated with their transfers. Critically, the TRA tool recognizes that it is one approach for conducting a transfer risk assessment – and that there are other ways for companies to carry out these assessments. We also appreciate the TRA tool's recognition that conducting such assessments can be a "complicated exercise" for organizations, particularly those with limited

resources, and its focus on the key issues of enforcing an IDTA and assessing the legal framework of the destination country.

In our view, two aspects of the TRA tool are particularly helpful:

- Its focus on helping companies identify the relevant parts of a destination country's legal framework. The TRA tool acknowledges that in assessing the potential risk of third-party access to data, companies need not look at the "whole regime" of a destination country, but instead "only those parts . . . which are relevant to your restricted transfer" helps companies focus their resources on the most relevant parts of the transfer assessment.[3] Similarly, the guidance emphasizes that a company's assessment should focus "not whether third party access, including surveillance, is permitted by local law, but rather whether the laws and practices include safeguards which are sufficiently similar in their objectives to the principles which underpin UK laws."[4]

- Its focus on the range of additional safeguards that companies can adopt to address potential risks. In particular, Table G identifies types and levels of measures that may supplement IDTA safeguards. We commend the ICO for identifying in this table a range of safeguards that reflect organizational and contractual measures, in addition to technical measures companies could adopt, and for recognizing that different levels of such measures may be appropriate in different circumstances, depending on the relevant transfer. We urge the ICO to continue updating Table G over time to expand the identified measures.

At the same time, we appreciate that the detailed nature of the TRA tool may also make it more burdensome for some companies to readily use the tool, particularly those without large compliance teams. For that reason, we encourage the ICO to consider issuing an executive summary of the TRA tool, which may create a practical way for companies of all sizes to easily identify the foundational questions involved in a TRA assessment. This sort of user-friendly executive summary could also cross-reference the full TRA, so that companies that want further details on one aspect could more easily interact with the larger amount of detail in the full TRA tool.

Finally, we encourage revisions that more expressly recognize that assessments may be performed for a set of transfers, such as the set of transfers involved in providing a particular product or service. Specifically, we encourage adding language to the introductory sections of the TRA tool that expressly recognizes the appropriateness of conducting a risk assessment

[3] TRA Tool, Page 5.
[4] TRA Tool, Page 4.

prior to commercializing or using a service that transfers the same types of data for the same purposes at scale.

Q10. Please provide suggestions for example transfer scenarios that we could include in the TRA tool.

Section 3: ICO model international data transfer agreements

Proposal 1: A new set of standard data protection clauses.

Background

The Information Commissioner has authority to issue a set of UK standard data protection clauses under UK GDPR in accordance with section 119A(1) DPA 2018.

Attached at Annex 2 is a new set of standard data protection clauses, (previously referred to as Standard Contractual Clauses (SCCs)), to be known as the model International Data Transfer Agreement (IDTA) under the UK GDPR.

We are consulting on this draft version of the IDTA in accordance with section 119A(4) DPA 2018.

Q11. Please provide us with your views on the draft IDTA, in particular:

- Does the IDTA provide effective safeguards for data subject rights?
- Is it clear how to use the IDTA in conjunction with the TRA?
- Does the IDTA provides a risk-based implementation of the UKGDPR and Schrems II?
- Will you will use it?
- How clear is the IDTA and how easy it is to understand?
- Would you prefer a modular approach, where you can select provisions, depending on whether the exporter or importer are controllers or processors?
- If the parties have incorrectly identified themselves as controllers or processors, should the right parts of the IDTA still apply to ensure there are appropriate safeguards? For example, if the importer is identified as a processor when a Court later decides it is a controller.

- Should there be an option to make changes to the Mandatory Clauses to remove sections which are not relevant (eg if the importer is a processor, to remove the controller obligations)?
- We have suggested that the Mandatory Clauses of the IDTA can be changed so that it can be used for a multi-party agreement, and that the ICO will produce a guidance version. Would you prefer there to be a formal multi-party IDTA?

Q12. At Chapter 5 of the IDTA, we are proposing to include a number of guidance templates including:

- optional TRA extra protection clauses;
- optional commercial clauses;
- a template to make changes to the IDTA;
- a multi-party IDTA; and
- an example of a completed TRA & IDTA.

Please identify any additional guidance templates that you would find helpful in the IDTA, and any TRA extra protection clauses and commercial clauses.

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

The ICO is considering issuing an IDTA in the form of an addendum to model data transfer agreements from other jurisdictions.

For example, model data transfer agreements have been issued by the European Commission, New Zealand and ASEAN (the Association of Southeast Asian Nations).

Q13. Please provide your views on this proposal. Is it helpful?

What is the economic value, or other value, of the ICO validating the use of these other model data transfer agreements?

Are there any other model data transfer agreements you would like us to consider?

BSA strongly supports the ICO's work to develop an IDTA in the form of an addendum to model data transfer agreements from other jurisdictions. We particularly welcome the example EU addendum included in the consultation, which would allow companies to amend the EU SCCs to work in the context of UK data transfers.

We encourage the ICO to continue this work, including to: (1) finalize the example addendum to the EU SCCs, so that companies may implement the IDTA by adopting this addendum, and (2) issue similar addendums to model transfer agreements in other countries, including in the future as other countries adopt such model transfer agreements. In these efforts, we encourage the ICO to focus on the creation of template addendums, which companies tailor and implement based on the actual transfers they are undertaking. This approach will provide companies with clear guidance on the appropriate substantive provisions for safeguarding data that are to be included in an addendum, without requiring companies to conform to the same strict format of document.

The approach of issuing IDTA in the form of an addendum is helpful because:

- *It is interoperable.* Companies that provide services in more than one country must identify – and implement – the additional privacy and data protection requirements imposed by another country's legal framework. Template addendums help companies do this efficiently, by listing those additional requirements which can then be mapped to existing legal obligations. This approach embodies the interoperable model companies strive for, while ensuring that organizations can readily identify and adopt measures to comply with each country's standards of data protection and privacy.

- *It is economically valuable*. Issuing an IDTA as an addendum is also economically valuable. This approach decreases cost of doing business in the UK, since it helps companies leverage the compliance work they have done for another country to comply with UK requirements. As a result, it may encourage more companies to enter the UK market than if those companies had to undertake standalone compliance efforts and enter into a standalone IDTA for each set of transfers.

- *It promotes global harmonization*. By recognizing the benefits of issuing model addendums, the ICO can establish a model that encourages data protection authorities in other countries to similarly issue addendums in support of international transfers, further supporting this interoperable approach to data transfers. Globally, several other regulators are considering adopting model contract clauses for cross-border transfers. The ICO's efforts can become a model for other regulators and help to

ensure model clauses can work together in practice to promote high data protection standards.

In addition to finalizing the addendum for the EU SCCs, we encourage the ICO to issue addendums for countries that have finalized their own model transfer agreements, such as New Zealand. We also encourage the ICO to closely monitor the creation of model transfer agreements in other countries that may be implementing a new national data protection law, such as Brazil, and to issue new UK addendums as such other model agreements are finalized.

The consultation also asks specifically for views on the addendum to the EU SCCs. As noted above, we strongly support finalizing this addendum, so that companies may rely on the addendum to comply with the IDTA's requirements.

As an example, attached at Annex 3 is a UK GDPR addendum to the European Commission SCCs. The addendum amends the European Commission SCCs to work in the context of UK data transfers.

Q14. Please provide your views on the addendum to the European Commission SCCs.

Please see the above response.

As noted in the above response, BSA strongly supports the ICO's work to develop an IDTA in the form of an addendum to model data transfer agreements from other jurisdictions. We particularly welcome the example EU addendum included in the consultation, which would allow companies to amend the EU SCCs to work in the context of UK data transfers.

Proposal 3: Disapplying the use of the Directive SCCs when the Commissioner issues an IDTA.

Background

Schedule 21 of DPA 2018 sets out "Further transitional provisions" for the UK leaving the EU. In particular, it allows for the continued use of the SCCs issued by the European Commission under the Data Protection Directive 95/46/EC (we refer to below as "Directive SCCs").

Schedule 21, Paragraph 7:

UK GDPR: transfers subject to appropriate safeguards provided by standard data protection clauses

1) Subject to paragraph 8, the appropriate safeguards referred to in Article 46(1) of the UK GDPR may be provided for on and after IP completion day as described in this paragraph.
2) The safeguards may be provided for by any standard data protection clauses included in an arrangement which, if the arrangement had been entered into immediately before IP completion day, would have provided for the appropriate safeguards referred to in Article 46(1) of the EU GDPR by virtue of Article 46(2)(c) or (d) or (5) of the EU GDPR.

The Commissioner may disapply those Directive SCCs.

Schedule 21 Paragraph 8.

1) Paragraph 7 does not apply to the extent that it has been disapplied by—

    (a) regulations made by the Secretary of State, or
    (b) a document issued by the Commissioner.

Q15. What are your views on when the Commissioner should disapply the Directive SCCs?

We propose: 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:

- at the end of three months for new Directive SCCs; and
- at the end of a further 21 months for all Directive SCCs.

This time period allows you to enter into new Directive SCCs for a further three months and so sign any Directive SCCs you have in train. But, you must have updated all your Directive SCCs within 24 months.

Please provide your views on this proposal. Please highlight any relevant privacy rights, legal, economic or policy considerations and implications.

The consultation also addresses the transition away from UK recognition of the EU SCCs, after issuance of the final IDTA.

It suggests a timeline for that transition based on when the new IDTA is

adopted, with the transition starting 40 days after the IDTA is laid before Parliament. After that time, the EU SCCs would be disapplied: (1) after three months for new SCCs, and (2) after an additional 21 months for existing SCCs.

We recommend two changes to this timeline:

- First, the timeline should be based on when the final IDTA template addendum to the EU SCCs is ready for adoption by companies, rather than only on when the new IDTA is laid before Parliament. This would ensure that companies currently relying on the EU SCCs can transition to the addendum version of the IDTA. As we noted at the outset, our companies find significant practical and economic value in implementing the IDTA through such an addendum – and the transition time should permit companies to transition from reliance on the EU SCCs to reliance on the IDTA addendum to the EU SCCs, without requiring them to first adopt the full standalone IDTA while the addendum is finalized.

- Second, and particularly if the IDTA addendum to the EU SCCs is not finalized at the same time as the IDTA, the timeline for disapplying EU SCCs to new contracts should be extended to six months, rather than three months. This would permit companies additional time to implement compliance practices aligned with the new IDTA.