ABI response to ICO consultation on International Data Transfers

October 2021

ABOUT THE ASSOCIATION OF BRITISH INSURERS

1. The Association of British Insurers is the voice of the UK's world-leading insurance and long-term savings industry. A productive, inclusive and thriving sector, our industry is helping Britain thrive with a balanced and innovative economy, employing over 300,000 individuals in high-skilled lifelong careers, two-thirds of which are outside of London.

2. The UK insurance industry manages investments of over £1.7 trillion, pays nearly £12bn in taxes to the Government and powers growth across the UK by enabling trade, risk-taking, investment and innovation. We are also a global success story, the largest in Europe and the fourth largest in the world.

3. Founded in 1985, the ABI represents over 200 member companies providing peace of mind to households and businesses across the UK, including most household names and specialist providers.

EXECUTIVE SUMMARY

4. We welcome the ICO's aims to support a proportionate and risk-based implementation of UK GDPR that maintains a high standard of data protection post-Brexit, not only for the protection of data but also to retain the high standards expected by trading partners across the world.

5. We also welcome the ICO's aims to open up more avenues for international data transfers but seek that any proposals for new avenues are able to work in harmony with mutual adequacy decisions, not least the UK and EU/EEA mutual adequacy decisions made earlier this year.

6. International data transfers are important for the insurance industry, necessary as part of outsourcing, reinsurance, data storage and other arrangements to fulfil underwriting, claims, risk management functions and to assist in the development of innovative new products and services for customers and business partners.

7. Whilst all parts of the consultation are of importance to our members, we have focused in our response on the high-level points affecting the insurance and long-term savings industry. We would be happy to engage further on this important issue.

RESPONSE

Transfer Risk Assessment (TRA)

Requirement for firms to assess local laws and customs

8. We have strong concerns about the requirement for firms to make their own assessment on local laws and customs:

    a) The importer is 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. This would be an issue in jurisdictions where importers do not have a UK presence within the enforcement scope of the UK GDPR.

    b) While firms can make their own assessment on the data being transferred and on the level of data protection and controls in place by the organisation to which the data is being transferred, firms would face significant challenges if required to are not in a position to be able to make an assessment on the local laws and customs of the third country in which the organisation is subject; any such assessment would be very costly in terms of the expertise and frequency of such expert input.

    c) Even if firms found the resources to carry out such assessments, there would likely be inconsistent results where it is assessed that the same jurisdiction has a different level of risk depending on which firm has carried out the assessment. For many companies, especially for SMEs that form part of a supply chain for insurance firms, a requirement to carry out such an assessment may be unworkable.

    d) We also note that the IDTA places the obligation on the importer to provide the information but does not specify the form in which this should be provided. As a result, there is a risk that the information may be in a format where the key information is not easy to extract and in a language that needs translation or interpretation. We seek clarity within the guidance to avoid this risk.

    e) We seek that the ICO (potentially in conjunction with DCMS) determines whether the local laws and customs of a third country are “sufficiently similar” to those of the UK. We believe it would be helpful if the ICO could create a list or map of countries and jurisdictions (together with any specific data protection legislation that the country/jurisdiction has adopted, the name of the Data Protection Authority where there is one in that country/jurisdiction, a note on whether that jurisdiction is deemed to be “sufficiently similar” and any other relevant information in the context of data transfers). CNIL has developed a map of data protection around the world, available on their website; it would be helpful if the ICO could publish a similar tool providing further detail on the local laws and customs as part of any toolkit to assist firms.

Complex transfers

9. The draft Transfer Risk Assessment and tool notes on page 8 that the TRA tool "is designed to assist…when making routine restricted transfers…and can only be used for those transfers which are not complex or high risk." The guidance states that firms will need to do more detailed risk assessment for transfers which are complex.

10. We wish to emphasise that many transfers can be complex in nature (for example involving elements of Artificial Intelligence), although not necessarily high-risk (for which the ICO recommends the completion of a more detailed risk assessment or relying on another appropriate safeguard or an exception).

11. We seek that the ICO includes guidance that specifically addresses and assists firms with the ICO's expectations for implementation of such complex transfers that do not fit into the category of either routine or high-risk transfers. This is an important area for clarity and is currently missing from the guidance. We would be happy to assist the ICO with the development of case studies and scenarios that would fall into such categories. We would also note that the TRA guidance would be easier to use if it was more concise, and also made available as an interactive tool.

International Data Transfer Agreement (IDTA)

12. The IDTA introduces a one-size-fits for all transfers, including a data transfer between processor and sub-processor (Part One Page 12 & 16.1.2). We believe it is important that the ICO provides a separate agreement IDTA for a data transfer between the overseas processor and sub-processor. We also believe it is important that the separate agreement provides the controller with the right to enforce against processors.

13. At Section 15**,** the draft IDTA requires the data processor to notify the data controller *if the processor's data breach is likely to result in a risk to the data subjects*, even if the breach has occurred with a combination of the controller's and processor's data. We believe that the processor must notify the data controller regardless of the level of risk because it provides an opportunity for the data controller to investigate and understand the issue and level of risk with the processor. This would enable the controller to take any necessary steps and help to mitigate or prevent any similar future issues. We would also note that controllers are currently obliged to maintain records of all breaches and the proposed wording would mean controllers would no longer be able to fulfil this obligation.

ABI concerns that proposed review timeframes of the IDTA are too frequent

14. We feel strongly that the proposed review timeframes of the IDTA, including the least frequent option of an annual review, are too frequent to be practicable or helpful to achieving an outcome of high standards of data protection. We propose the review timeframes of the IDTA be determined on a risk basis or otherwise upon a material change.

Interaction between Restricted Transfers and GDPR

15. We are seeking clarity on requirements for both controllers and processors in the context of data transfers back to the UK, as well as clarification on how this would fit with the GDPR.

16. In the context of transfers from one legal entity to another, we are concerned that there is no extra safeguard required. This seems to reduce the level of protection provided to data subjects and may reduce awareness and level of accountability within international corporations.

<u>Consultation document</u>

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

17. We are seeking that any requirements in relation to territorial scope are clearly defined to both UK and overseas firms; any uncertainty will lead to protracted (and therefore more costly) negotiations between UK firms and the overseas firms with whom they contract.

18. We would value further ICO guidance, including case studies and other examples to aid firms' understanding of the different roles of controllers, processors, joint controllers, sub-processors etc.

Disapplying the use of the Directive SCCs when the Commissioner issues an IDTA

19. The consultation seeks views regarding the timing for the disapplication of the existing Directive SCCs. The ICO proposes:

    "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) (ii) 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."

ABI request for longer transition period to implement changes

20. We urge the ICO to provide a longer transition period to enable organisations to implement the required changes. This is of particular importance where complex contractual arrangements are already in negotiation, where arrangements to conclude contracts are in-flight and where existing contracts have a timeframe that straddle the different sets of SCC requirements. On a practical level, the changes affect not only legal teams but a range of other roles and disciplines, which will require adequate time to coordinate and resource.

Terminology

21. We would welcome clarity on some new terminology, including:

    a) "Any reasonable request". This is ambiguous and we are seeking guidance on what this means, perhaps including some case studies from a range of sectors to illustrate examples.

    b) "low risk": We would welcome further guidance and examples on what the ICO regards as being "low risk".