Association of British Insurers – Written Evidence (DAT0014)

House of Lords Call for Evidence: Data adequacy and its implications for UK-EU relationship

Overview

1. With the upcoming June 2025 deadline for a renewal of the EU's UK data adequacy determination, and the ongoing passage of the Data Protection and Digital Information Bill, we welcome the Committee's timely inquiry. We hope this short response is helpful for the Committee's evidence.

2. The most legally sound and stable way to transfer personal data between the UK and the EU27/EEA destinations is, without question, for mutual data-adequacy decisions between the EU and UK. While the UK, rightly, did not place a time limit on its decision, we hope that the last 5 years have demonstrated to the European Commission that the UK has not disregarded the rulebook following Brexit, and that it continues to maintain significantly high standards of data protection. Consequently, we would not only wish to see a positive renewal of the decision made by the European Commission in 2021, but that it can feel confident in taking a decision for the long term, and one that is in line with data adequacy decisions it has granted to other third countries where there is no cut off point/renewal clause.

ABI Response:

3. Data flows between EU and UK underpin the services economy and are vital for almost any business with customers, suppliers or operations in both the EU and UK. For data to continue to flow freely between the EU and the UK, the European Commission needs to decide whether the UK (as a third country) has a level of data protection that is sufficiently robust, or "adequate". Whilst adequacy is the EU's way of protecting the rights of EU citizens by insisting upon a high standard of data protection in foreign countries where their data will be processed, the UK has implemented and maintained the same high standard of data protection as the EU, as set by the GDPR.

Digital and global economy

4. A strong, robust and trusted data protection regime is a key part of a strong digital economy and crucial for innovation. It is beneficial for all countries to have a common framework and standards to avoid

fragmentation. The GDPR has raised the bar for data protection across UK and EU. Internationally, the GDPR has also been closely replicated in laws across the world as a consistent, trusted standard for data protection. As data protection laws become stronger and regulators get more enforcement powers globally, we believe it is important that the UK retains its high standards of data protection, not only for the protection of its citizens but to retain the high standards expected by trading partners not only within European Union but across the world.

5. For the (re)insurance industry, data is a core part of business, used to price and underwrite all kinds of risks to reflect a customer's particular circumstances as accurately and fairly as possible (driving a car, travelling abroad, starting and running a business, providing for life after work) to provide cover that best meets their needs, and to handle and validate claims. It also provides useful insights that can help to optimise processes, understand customers' needs and provide new solutions. There are many instances in which insurers may need to transfer data across borders, including:
   - within a Group that operates globally or across a number of jurisdictions
   - as part of outsourcing arrangements
   - as part of reinsurance arrangements
   - as part of commercial engagement
   - as part of data storage arrangements, including servers and cloud services.

   to an international organisation. An international organisation is defined as "an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis or, an agreement between two or more countries" (GDPR Article 4).

The UK should pursue an adequacy decision

6. As mentioned above, the most legally sound and stable way to transfer personal data between the UK and the EU27/EEA is through mutual adequacy decisions by the European Commission and the UK. Without adequacy decisions between the UK and EU, alternative but less attractive and less practical options will be required to ensure continuing data flows. Potential options include localising data centres, (invoking data residency) and obtaining relevant authorisations and putting in place available arrangements within GDPR Chapter V that enable third country data transfers. However, these are all less robust

and cover fewer situations than a data adequacy decision. For example:

- **Consent** can be withdrawn or withheld at any time, making it unreliable for important activities like financial crime prevention
- **Binding Corporate Rules** are valid for intercompany personal data transfers only. They are only available to companies with a presence in an EU Member State and not a feasible solution for smaller firms who do not have a group-level presence. The UK Information Commissioner recently amended the process to allow an Addendum approach to already established EU BCRs to support UK organisations who have established EU BCRs. The UK standalone BCR application process is bureaucratic and expensive with limited success for applying UK organisations post Brexit.
- **Standard Contractual Clauses** are more flexible but may provide less legal certainty, and have been subject to legal challenge in recent years (e.g. Schrems II). In addition, the identification and renegotiation of relevant contracts can be time-consuming and complex and financial costs to organisations are significant.
- **Legitimate interests derogation** has a limit on the size and frequency of transfers, coupled with a requirement to notify the Data Protection Authority and the data subject, which makes this unworkable for most arrangements or transfers, and unlikely to be sufficient for Special Category data.

7. If the UK's adequacy decision is not renewed, this could result in a significant increase in compliance burdens for business in the UK and EEA. There will also be increased costs particularly in relation to putting new measures in place and maintaining them, and a period of legal risk and uncertainty until this is completed.

8. Uncertainty surrounding the transfers of personal data will create significant challenges for the growth and development of the digital economy, uncertainty for electronic personal data flows which are so essential in the online world, and for businesses offering services beyond the UK.

UK and EU citizens

9. Restricting the free flow of personal data between such close neighbours, could have serious implications for citizens if something goes wrong while abroad. For example:

Scenario 1 – UK traveller to the EEA admitted, unconscious, to an EEA healthcare provider, concerned about GDPR compliance without data adequacy, delays transferring the UK traveller's personal data to a UK travel insurance provider.

- this same issue would seem to apply for travel insurance for a UK customer travelling outside of the UK. E.g India. An insurer would transfer data needed to deal with the claim (either to the data subject or the Indian healthcare provider). The legal basis would be necessity for contract (Ar49.1) and if health data the insurance derogation under DPA 2018 would apply.
- If the customer is unconscious, the EEA healthcare provider would not necessarily know which insurer to contact unless they found details of an insurance company in the personal possessions of the customer or if a relative of the customer provided information to the EEA healthcare provider. In this case, insurers anticipate that the healthcare provider might be able to rely on vital interests but the assessment of how this threshold is met could vary. There could be some tension between the vital interest that the patient is treated, and the healthcare provider wanting assurance that they will be paid for the treatment, and the EEA health provider ensuing that the individual's data is protected in line with GDPR requirements.
- Ensuring the fee flow of data and allowing the healthcare provider to not have to consider whether they have a legal basis, mitigates against delays which could be detrimental to the patient.

Scenario 2 – EEA travel insurer having to transfer personal data to a UK healthcare provider where there is an unconscious customer of the EEA insurer admitted to the UK healthcare provider. Would the EEA travel insurance provider delay transferring personal data back to the UK healthcare provider, while they consider the legal risk of GDPR?

- The insurance provider will ordinarily obtain information from the healthcare provider, not provide it, unless the insurer happened to have health data that would be very relevant for the treatment (e.g. allergic to penicillin) in which case "vital interests" might be relied on.
- Where normal personal data (not special category data) needed to be transferred by the EEA insurer to the healthcare provider, insurers would anticipate that they could rely on necessity for contract.
- Insurers noted the following cases where insurers may need to provide information to the healthcare provider:

- Guarantee of payment: the insurance provider may guarantee payment to the hospital on an insurance policy (there is not much sensitive or personal data in that – it is more of a financial reassurance for the hospital that they will be paid for the care they give)
- The insurance provider may tell the hospital of logistical plans to move the patient (such as an assisted repatriation home by Air Ambulance).

- If free flow of data is no longer permitted, there may be delays in providing essential services which could be of detriment to the patient. However, it is primarily a burden on the healthcare provider to ensure that they comply with Chapter V of GDPR, because they would hold most of the information necessary to settle the claim. Transfers from the insurer are secondary or consequential and are based on the dataset that would have been made available by the healthcare provider. Their transfer will usually rely on or match the lawful ground established by the healthcare provider.

Data Protection and Digital Information Bill

10. The insurance and long-term savings industry recognises the Government's overall ambition to set a globally competitive framework on data protection, which enables innovation and preserves high standards. For the ABI's members though, it is essential that the proposals in the Bill maintain data adequacy internationally and ensure that the new regime does not introduce inefficiencies and complexity for firms operating across jurisdictions, which could undermine our international competitiveness. Members are aware that changes within the Bill which could affect the ICO's regulatory independence may have a negative impact on the EU's decision to renew the UK's data adequacy and should be addressed.

11. A number of proposals will require supporting ICO guidance to ensure the new requirements are clear and practicable. For example, we would welcome a commitment for supporting ICO guidance on proposals including in relation to vexatious or excessive requests by data subjects, on automated decision-making, and on what the Government expects firms to consider in relation to "... traditions and culture of the country or organisation" within the new Article. 45B data protection test. The rest of the list of factors seems to align to existing guidance on carrying out transfers impact assessment (e.g. human

rights records, powers of enforcement authorities etc.) but this wording is new.

12. With the new definitions of personal data it would be essential for prudent supplier management for clarification to be provided, during the legislative process and through ICO guidance, on where firms further down the supply chain are no longer considered to be directly processing personal data and therefore no longer subject to the primary Controller's oversight. Firms have also raised that AI, machine learning and actuarial science could all be potentially considered as "scientific". There is concern that such a broad brush definition could have unintended consequences on consumer confidence in these technologies and their use within the financial services system. Additional guidance around applying all of the new definitions would be welcomed.

13. For firms operating in a multi-jurisdictional environment, many proposals provide limited scope for efficiency and the benefits to firms and customers are unclear. Indeed, we believe that these proposals may have the unintended consequences of adding compliance costs for firms and members have expressed concern about potentially burdensome new requirements. Proposals regarding the Senior Responsible Individual are likely to cause unnecessary burdens for UK businesses who have already established an approach to compliance with GDPR through the appointment of a DPO. To ease this burden, Bill should be amended to state that firms can 'either appoint a Senior Responsible Individual or utilise a DPO that is already in place where GPDR requirements for that appointment were met. It is important to be aware that the Senior Responsible Person does not have the same independence of the DPO and there could be easily a conflict of interest which could override the interests of the data subjects.

14. We would highlight in particular the proposals regarding the Senior Responsible Individual, assessment of high-risk processing and record keeping. Both are examples of prudent risk management for firms and support effective Data governance. There is opportunity to simplify records management obligations in the Bill from GDPR. Obligations should be kept but in a simpler and less prescriptive format than currently under GDPR. We welcome further engagement with DSIT and the regulators on the proposed obligations and how they will be implemented.

Association of British Insurers

Received 9 May 2024