UK Finance – Written Evidence (DAT0020)

UK Finance input to the inquiry

UK Finance represents over 300 firms within the financial services sector. Our objectives are to support industry to drive innovation and economic growth, assist vulnerable customers, combat economic crime, and facilitate the transition to net zero.

The inquiry is focused on four themes. In our response we aim to provide succinct input focused primarily on two of these themes. In summary, we strongly support the maintenance of 'mutual adequacy decisions' between the EU and the UK, which underpin continued free data flows between the two jurisdictions. These data flows are a key support of commerce between the UK and the EU.

We note that there is uncertainty over exactly what the limits and thresholds are in practice for a jurisdiction to pass the GDPR's adequacy tests. Furthermore, although a technical decision in theory, in practice adequacy determinations are also likely to be political. As such, it is important for the Government to maintain ongoing, regular and transparent dialogue with EU stakeholders to provide reassurance, debunk any myths about the UK reforms, and to identify and address any areas of high risk. This dialogue could helpfully produce public documentation to increase clarity and predictability for businesses and other stakeholders.

We further recommend that the Government continue to engage with stakeholders internationally – including the EU – to further develop mechanisms for secure and trusted international data flows. There is potential, for example, to build on the network of countries that the EU has deemed 'adequate', and on the Global Cross-Border Privacy Rules Forum.

If you have further questions, please contact Walter McCahon (Principal, Privacy and Data Ethics) at: walter.mccahon@ukfinance.org.uk.

The value of UK adequacy and implications of a disrupted or revoked UK-EU data adequacy scenario

At present, UK financial services firms are closely connected with EU firms. These relationships require ongoing transfers of personal data back and forth.

In addition to transfers between firms and their clients, there are data transfers between separate legal entities within the same group. Many financial services firms operate regional or global 'hubs' where specialised data processing is done for firms across the group. Examples include 'know your customer', crime detection, HR or specialist customer service functions. The entities in these hubs receive customer and employee data from many jurisdictions. Similarly, firms operate centralised data centres and regional cloud data centres for use by group entities in multiple jurisdictions.

Separately, business groups transfer data across borders to manage risk more effectively. For example, firm entities share data on customers in order to have a complete picture of customer activity across jurisdictions ('single customer view').

Finally, many firms utilise service providers in other jurisdictions that provide specialist services, such as HR platforms and payroll systems.

In the absence of mutual adequacy decisions between the UK and the EU, firms will need to 'repaper' these relationships. Under Chapter V of the GDPR – UK and EU versions – in most cases this is likely to involve a bureaucratic process of preparing and signing 'standard contractual clauses'.

An alternative for intragroup transfers – but not transfers to non-group entities – is to set up 'binding corporate rules' and have these approved by the ICO and EU authorities. The approval process, however, has historically taken many months, on top of the time needed to prepare the documents and go through the internal governance and approvals at each relevant legal entity. Indeed, we understand that some firms' experience is for regulatory approvals to take several years.

Practical impacts

As with international trade agreements and similar treaties, firms can do business across borders without a political framework such as 'adequacy'

in place. However, this would be with added costs, inefficiencies and risks, potentially impacting UK competitiveness. Depending on the geographical footprint, business model and structure of the firm in question, putting in place alternative arrangements could involve thousands of contracts to review and amend. This is a time-consuming process likely to cost millions of pounds and take hundreds of hours of time.

As noted above, setting up binding corporate rules is a very lengthy process.

In addition to revising legal arrangements, firms may also choose to move some data processing centres – where these process EU data – from the UK to EU countries in order to de-risk.

In some instances, firms may need to simply exit relationships with service providers and clients.

There is also a risk of significant business disruption, particularly if the loss of adequacy happens unexpectedly or suddenly. If firms do not have time to put in place alternative legal means of transfer, there is a risk that certain relationships and processing operations will need to be frozen or discontinued. Smaller firms may find the disruption particularly difficult to manage.

Beyond immediate business impacts, the loss of UK adequacy would also risk impacting the UK's global reputation as a digitally connected country and a safe destination for data. And there may also be risks to consumer confidence and trust in the digital ecosystem.

In turn, these broader impacts may impact firms' risk assessments and business decisions. Adequacy decisions provide reassurance that data will be treated in a manner meeting minimum data protection standards; this assurance is likely to increase in importance as the ubiquity of digital technologies grows. If the UK were to lose adequacy, this could impact the sentiment of European (or indeed global) customers and partners, increasing pressure on firms to move data processing out of the UK and reducing the international attractiveness of UK providers.

Specific financial sector risk

A key consideration for financial services is what the loss of UK adequacy might mean for the UK's ongoing access to the Single Euro Payments Area (SEPA) and the associated ability for payment service providers to

offer efficient euro retail payment services to UK consumers and businesses.

SEPA was created to fully harmonise electronic euro payments to make it as easy and convenient for consumers and businesses to pay across Europe with one payment account as it is in their home countries. The European Payments Council (EPC) – in which the UK is represented and engaged – manages the SEPA payment schemes covering euro credit transfers, instant payments and direct debits. The EPC plays a role in defining the geographical scope of SEPA, which currently covers the 27 EU Member States plus the United Kingdom, Iceland, Norway, Liechtenstein, Switzerland, Monaco, San Marino, Andorra and Vatican City State/Holy See.

The EPC's SEPA participation criterion (c)(iii) requires of participant countries that: "The transfer of data to any of the Applicant's institutions by a SEPA Scheme participant would not create any legal or regulatory issues for such SEPA Scheme participant (for example, under the applicable data protection laws)." We note that EU GDPR also allows transfers of personal data out of the EU by means of standard contractual clauses or other safeguards, as outlined above. Nonetheless, there is a risk that loss of UK adequacy could cast doubt on the UK's satisfaction of this criterion and put SEPA access at risk for UK institutions.

Possible challenges to UK-EU data adequacy regime

Overall, we support the Data Protection and Digital Information (DPDI) Bill, and its objective of reducing burdens and facilitating innovation while maintaining strong protections for personal data. However, there are some provisions that – while not 'smoking guns' – amount to *potential* challenges when arguing the UK has retained sufficient alignment with GDPR, and which merit consideration from a UK adequacy perspective

We note that the DPDI Bill will not pass ahead of the 2024 election and is therefore not immediately relevant. However, the Bill may resurface in some form and the overarching issues will remain relevant to the renewal of UK adequacy in 2025. As such, we nonetheless include the following analysis and discussion in relation to the latest draft of the Bill before the election was called:

- ICO independence – having an effective independent regulator is a key criterion for adequacy under GDPR Article 45(2)(b). We note that in the design of the DPDI Bill there were proposals that would have created a risk of materially reducing the ICO's independence. However, the latest version of the Bill appears to have largely resolved this challenge, for example by removing the Secretary of State's veto power over statutory codes, and ensuring that the Information Commission's board of directors selects the chief executive, rather than the Government. There are new powers for the Government to set secondary goals for the Information Commission, but these remain subsidiary to its privacy-focused primary objectives. These more balanced reforms or ICO governance should be supported.
- Surveillance and public authority data access –
    - Surveillance and public authority data access issues are likely to be a key area of interest for the review of UK adequacy. "The access of public authorities to personal data" is one factor the European Commission must consider under GDPR Article 45(2)(a) and the issue is referenced in the summaries of adequacy decision reviews published by the European Commission. Furthermore, we note that this was a central consideration in the 'Schrems II' decision of the Court of Justice of the European Union, which invalidated the limited EU-US adequacy decision known as Privacy Shield.
    - In the lead up to the UK leaving the EU, the UK's state and law enforcement surveillance powers were seen as a particular adequacy risk, in light of court decisions such as *Watson*.[1] However, the creation of the Investigatory Powers Commissioner's Office and strengthening of the safeguards applying to law enforcement and intelligence services use of data collection powers via the Investigatory Powers Act 2016 strengthened the UK's regime, as recognised by the UN Special Rapporteur on the Right to Privacy in 2018.

[1] See for example the 21 May 2021 European Parliament resolution on UK adequacy, paragraphs 12 – 17. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0262

- These positive changes made to the frameworks governing UK authorities' data access mitigate the data adequacy risks. However, there is a risk of the UK being seen as akin to the United States and being subjected to greater scrutiny in any future adequacy review or legal challenge. We further note changes contained in the DPDI Bill that – while not completely analogous to the law enforcement and intelligence powers that were overturned previously – do have certain parallels.
    - The first paragraphs in both Schedule 1 and Schedule 2 of the DPDI Bill create together a new ability for firms to freely disclose personal data to public authorities, where the authority claims the data is necessary in the public interest. This provision removes the prior requirement for the firm to establish its own legal basis when asked to voluntarily disclose personal data[2],involving an assessment of impacts on individuals (the 'balancing of interests' test). We understand that these provisions are intended to address such situations as where authorities need rapid access to data to track a pandemic, but they are not limited to such purposes in the Bill. They therefore seem to create a broad way for authorities to acquire the personal data of people in the UK, in principle including bulk personal data for enforcement purposes, which could resemble 'fishing'. And these provisions lack the safeguards that normally sit around the use of binding data acquisition powers, such as clear criteria for legitimate use, or requiring external judicial approval before issuing a data request. We are uncertain of whether this in fact poses a material risk to UK adequacy, but we do note parallels with the surveillance cases above. This data acquisition gateway is also much wider and contains fewer safeguards than the provisions in Chapter V of the EU Data Act which are intended to achieve a similar aim (for example, Article 16(2) of the EU Data Act does not allow use of the

[2] As opposed to compliance with a production order or similar binding data request.

powers for law enforcement purposes). These provisions may therefore warrant consideration as potential risks to UK adequacy. We have previously suggested the addition of limitations and safeguards to this provision of the Bill.

- We further note the creation of new powers for the Department of Work and Pensions (DWP) under clause 128 and Schedule 11 of the DPDI Bill, enabling acquisition of bulk personal data from firms. We understand these powers are intended to enable DWP to more effectively tackle fraud and error in benefits payments. However, we note that – under the latest draft of the Bill – the purposes to which the data can be put are not limited to this under paragraph 5 of new Schedule 3B to the Social Security Administration Act 1992, created by Schedule 1 of the DPDI Bill. Furthermore, there are no clear criteria for when the powers can be used or regarding what information can be obtained, there is no requirement to seek an external authority's approval to invoke the powers, and there is no external oversight; the Secretary of State appears to have broad discretion as to their use and scope under paragraph 1 of new Schedule 3B. Again, we are not certain whether this provision poses a risk to UK adequacy, but it may warrant consideration. We continue to discuss this provision with Government.

- The proposed new "data protection test" under new Article 45B of UK GDPR (as set out in Schedule 5 of the Bill) may be of concern to the European Commission. This test requires that third country protections are "not materially lower [than those offered in the UK]". This is a requirement that the Government must be satisfied of before deeming another jurisdiction adequate from a UK perspective, and a requirement firms must be satisfied of when making transfers to non-adequate countries using other transfer safeguard mechanisms such as standard contractual clauses. However, this new test does not require 'essential equivalence' as required under EU law, following the Schrems I court case, which invalidated the Safe Harbor adequacy decision. Although the UK

drafting clearly has the same general policy intent as the 'essential equivalence' test, it could be taken to be weaker. Furthermore, the EU GDPR does specifically mention the 'rules for onward transfer of personal data' as a key consideration for adequacy decisions in Article 45(2)(a). As such, the European Commission may have concerns in relation to onward transfers of EU data subjects' personal data from the UK. UK-EU coordination in relation to potential adequacy third country decisions may be valuable in future to provide reassurance.

- The proposed change to the definition of 'personal data' in clause 1 of the Bill will mean that some data currently defined as 'personal' may no longer be considered personal data under UK GDPR, and so will be excluded from the protection afforded by UK GDPR and the Data Protection Act 2018. There is also potential for what is considered 'personal data' to change depending on who is doing the processing of a given dataset. Under the new definition, whether data is considered 'personal' will sometimes depend on the cost, time, effort and resources required to identify individuals. These factors will vary from firm to firm so there will be more scope for a given dataset to be subject to GDPR safeguards when processed by one firm but not when processed by another.
- Clause 9 inserts a new Article 12A into UK GDPR. This allows data controllers to charge a fee for, or to refuse to act upon, data subject access requests that the data controller considers 'vexatious or excessive'. This replaces the GDPR standard for refusing requests that were 'manifestly unfounded or excessive', thereby potentially impacting the rights of individuals if this is taken to be a lower bar.
- Clause 14 of the Bill amends the current provisions on automated decision making (ADM). Currently there is a prohibition on decisions made solely by automated means which have a legal or similarly significant effect on the individual, subject to some exceptions. There are also safeguards required when ADM is permitted under an exemption, including a right to information about the ADM and a right to request a human review of decisions. The new provision in the DPDI Bill limits this prohibition to automated decision-making based fully or partly on the processing of special category data (e.g., race, health information, ethnicity or sexuality). The new

provision does still require firms to have similar safeguards in place in order to use relevant automated systems but the initial prohibition is removed. We consider the safeguards and approach in the DPDI Bill to be proportionate, but this change may nonetheless raise concerns for European stakeholders. We note that countries whose adequacy decisions were recently renewed – such as Canada and New Zealand – have no specific ADM rules, but we nonetheless suspect that ADM will be an area of interest in relation to the UK.

- Finally, we note that the approach to regulating AI in the UK is quite different to the prescriptive approach of the EU. This may ultimately raise concerns if the European Commission links AI regulation to data protection adequacy decisions, although the risk may be mitigated in part by the EU AI Act's extraterritoriality provisions.

It is difficult to assess the risk of the UK losing adequacy. Although existing adequacy decisions have been renewed despite significant differences with the EU GDPR, more attention may be given to some considerations in relation to the UK's adequacy status than to others' (see for example our comments above regarding ADM). We suspect that there is a non-negligible risk of losing adequacy and encourage Government to maintain ongoing, regular and transparent dialogue with EU stakeholders to provide reassurance, debunk any myths about the UK reforms, and to identify and address any areas of high risk.

ENDS

Received 24 May 2024