HOUSE OF LORDS
European Affairs Committee

House of Lords
London
SW1A 0PW

Tel: 020 7219 6083
hleuroaffairs@parliament.uk

Rt Hon Peter Kyle MP
Secretary of State for Science, Innovation and Technology,
Department for Science, Innovation and Technology,
100 Parliament Street,
London,
SW1A 2BQ

22 October 2024

Dear Secretary of State,

UK-EU data adequacy

This letter sets out the key conclusions and recommendations which the House of Lords European Affairs Committee draws from our recent inquiry into UK-EU data adequacy.

In launching our inquiry in March 2024, we had very much in mind the expiry in June 2025 of the European Commission's current two decisions which award EU data adequacy status to the UK, under the EU General Data Protection Regulation (GDPR) and Law Enforcement Directive (LED). Our inquiry sought to explore, among other matters, the utility of the current UK-EU data adequacy arrangements, the challenges they might face, and the implications if the UK's adequacy status was lost. Given the remit of our Committee, our inquiry necessarily focused on data adequacy in the UK-EU context, but it raised wider international issues which we also addressed. We note that the House of Lords International Agreements Committee is conducting an inquiry into data and digital trade which covers international issues in more detail.

We held seven evidence sessions and received 21 written submissions, but were not able to hold a final evidence session with the then-Minister and to produce a report before the summer recess, given the timing of the General Election. Now, the political context has changed significantly — in particular, the previous Government's Data Protection and Digital Information Bill (DPDI Bill), which was the focus of much of our evidence, fell at dissolution. Nevertheless, the June 2025 expiry of the UK's EU adequacy status still looms, and the Government plans a Digital Information and Smart Data Bill covering some of the same issues as its predecessor's DPDI Bill.

We therefore judge that our key conclusions and recommendations, set out below, remain relevant, and could usefully inform the Government's new Bill and its engagement with the European Commission on the adequacy renewal process.

We bring the following Conclusions and Recommendations to your attention.

The UK-EU data adequacy regime since 2021: Should the UK seek to retain EU adequacy status?

a) Losing EU data adequacy status would impose significant extra costs and administrative burdens on businesses and public-sector organisations which share data between the UK and the EU, including law enforcement agencies and the NHS. It would raise new barriers to international trade and economic cooperation, and to trust in the UK's digital economy, running counter to the Government's objective of boosting economic growth. Losing adequacy would also have an adverse impact on Northern Ireland under the Belfast/Good Friday Agreement and the Windsor Framework agreement with the EU.

b) We heard a range of estimates of the economic value of retaining data adequacy, but all were substantial. We conclude that adequacy reduces administrative burdens and compliance costs, increases legal certainty, makes the UK a more attractive location for investment, and supports digital growth. The Government should therefore pursue data protection policies that are aimed at retaining the UK's data adequacy status with the EU, under both the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED). Securing adequacy renewal decisions from the European Commission in the first half of 2025 should be the Government's immediate data protection policy priority.

c) To limit uncertainty, the Government should engage early with the European Commission and other EU stakeholders with a view to ensuring that the adequacy renewal process is on a positive track, and providing reassurance as soon as possible about the retention of adequacy status. In this context, we welcome the call you held on 16 September with the European Commissioner for Justice. The Government should also explore the prospects for securing future adequacy renewal decisions from the Commission which do not expire after a fixed period, as is the case with the EU's other data adequacy arrangements.

d) The retention of GDPR after Brexit was beneficial in that it allowed EU-UK data flows and existing data protection processes to continue without interruption. However, the GDPR regime is far from perfect, and in several respects, problems remain with the legislation, its level of prescription, and its interpretation and implementation in the UK, which continue to create regulatory uncertainty for organisations. While compliance with GDPR can itself be costly, the loss of data adequacy would also lead to significant financial penalties for many organisations.

Risks to the UK's adequacy status

e) There are two distinct EU institutional risks to the continuation of the UK's adequacy status: the European Commission's adequacy renewal decisions for the UK in 2025; and the possibility of a legal challenge to Commission adequacy decisions in the Court of Justice of the EU (CJEU). Of these two risks, a successful challenge to the legality of Commission decisions before the CJEU is more likely than a Commission decision not to renew the UK's adequacy status.

f) When the Commission decides in 2025 whether to renew the UK's adequacy status, it is likely to give significant weight, alongside legal and technical issues, to wider political and economic factors. It is therefore essential that the Government takes this into consideration as it approaches the adequacy renewal process.

g) Given the economic benefits that also flow to the EU, the European Commission seems highly likely to want to renew the UK's adequacy status in 2025. It is therefore in both the UK and the European Commission's interests to ensure, to the extent that it is possible, that UK-EU data arrangements are compatible with the CJEU's case law. The Government should work with the Commission to this end. It should bear in mind that the Commission and European Parliament scrutinised closely the previous Government's Data Protection and Digital Information Bill. The Government should engage with the Commission and other EU stakeholders, in good time, in order to explain and provide reassurance with respect to any planned data protection reforms, in particular in areas such as the independence of the Information Commissioner's Office and any new role for Ministers to add new grounds of 'legitimate interest' for data processing. The Government should engage with the Commission similarly with respect to any changes in other relevant areas such as the Investigatory Powers Act.

h) The Government should approach the renewal of the UK's adequacy status as part of its wider 'reset' of relations with the EU.

i) The Government should develop its policies on data and data-related matters taking account of the potential implications for the UK's adequacy status. It should aim to maintain high data protection and privacy standards which are also in line with other important international standards such as the Council of Europe's Convention 108 on data protection. In its response to this letter, the Government should update us on the UK's status with respect to the Protocol amending the Convention, which the UK has signed but not yet ratified.

j) There is scope for beneficial reforms to the way in which the UK GDPR is currently operating, particularly regarding its cost to businesses, which would not necessarily jeopardise the UK's adequacy status. In this context, in preparing its Digital Information and Smart Data Bill, the Government should take account of the amendments to the previous Data Protection and Digital Information Bill which were adopted before the Bill fell at dissolution.

Wider international data protection policy

k) There is an active debate among policymakers around the world about the nature of future arrangements for international data flows with appropriate and feasible privacy safeguards. Adequacy may be coming under increasing strain as the basis of any international data protection regime, owing to its limited ability to scale across many jurisdictions and the political dimension which the process inevitably brings.

l) The UK is in a unique position with respect to international data protection policy. It is an associate member of the emerging Global Cross-Border Privacy Rules (CBPR) system and has strong historic connections with several of its members, including in APEC. Among CBPR members and associates, it also has the most experience dealing with, and a data protection regime that is closest to that of, the EU. There is an opportunity for the UK to act as a trusted and responsible data bridge. The Government should be fully engaged in the international debate about future data protection arrangements with the aim of ensuring that the outcome serves UK interests, in enabling digital innovation, and rights and protections the public expect to be in place.

m) In finding the right balance between the European and international regimes, we urge the Government to be mindful of the ways in which its international data protection policies may be a

risk to the UK's EU adequacy status. Without undermining its position in international fora, the Government should also aim to keep the EU institutions informed about its broad objectives and initiatives.

We would be grateful for a response to this letter within a month.

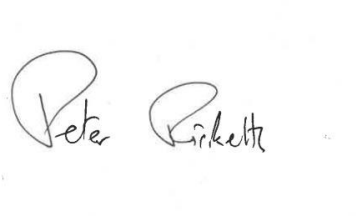
We also wish to invite you to give evidence to us on the issues raised by our inquiry which are dealt with by your Department, in the coming months while the adequacy renewal process is still in its early stages. We are pursuing separately an evidence session with the Home Secretary to discuss the law enforcement aspects of our inquiry.

We are aware of our responsibilities to publish the evidence on which our conclusions are based, do justice to the contributions of our witnesses, and inform wider debate on these issues, which are crucial for Britain's prosperity and security. The remainder of this letter therefore comprises, as appendices, summary background information on data adequacy and the UK-EU data adequacy regime (Appendix A); and a summary of the evidence we received (Appendix B). Our conclusions and recommendations above relate to the relevant sections of supporting evidence in Appendix B.

Finally, we would like to thank all those who provided evidence, and our specialist adviser Steve Wood.

I am copying this letter to Rt. Hon. Nick Thomas-Symonds MP, Paymaster General and Minister for the Cabinet Office (Minister for the Constitution and European Union Relations); Rt. Hon. David Lammy MP, Secretary of State for Foreign, Commonwealth and Development Affairs; Stephen Doughty MP, Minister of State (Europe, North America and Overseas Territories), Foreign, Commonwealth and Development Office; Rt. Hon. Yvette Cooper MP, Home Secretary; Rt. Hon. Douglas Alexander MP, Minister of State (Minister for Trade Policy and Economic Security), Department for Business and Trade.

Yours sincerely,



Lord Ricketts

Chair of the European Affairs Committee

APPENDIX A: DATA ADEQUACY: BACKGROUND INFORMATION

What is data adequacy?

Adequacy is a legal mechanism that allows the transfer of personal data from one jurisdiction to another (or the granting of access to data in one jurisdiction to organisations in another), while maintaining data protection standards set by the home jurisdiction.

In a jurisdiction that operates an adequacy system, domestic legislation empowers a government or other authority to grant adequacy status to another jurisdiction. If jurisdiction A grants adequacy status to jurisdiction B, a company or other organisation that is subject to the law of jurisdiction A can lawfully transfer personal data to a company or organisation in jurisdiction B as if that organisation were in jurisdiction A, without any additional safeguards or measures above those required for transfers within jurisdiction A. An adequacy decision applies only to the personal data that is covered by the legislation under which the adequacy decision is made. An adequacy decision may further specify that it applies only to transfers made for certain purposes or to certain sectors or types of organisations.

Adequacy is only one of several legal mechanisms that allow the transfer of personal data between jurisdictions with safeguards for data protection. The principal alternatives to adequacy are:

- Standard Contractual Clauses (SCC). These are issued by the relevant authority in the home jurisdiction and are signed up to by both parties to a data transfer.
- Binding Corporate Rules (BCR). These may be used for international transfers within a single corporate group. They must be approved by the relevant authority.

How does the EU data adequacy system work?

EU data protection law extends to the European Economic Area (EEA); when the European Commission acts under EU data protection law, it does so for the whole EEA.

Two pieces of EU law authorise the European Commission to adopt adequacy decisions with respect to third countries:

- the General Data Protection Regulation (GDPR), which does not cover criminal law enforcement;[1] and
- the Law Enforcement Directive (LED), which covers only criminal law enforcement.[2]

[1] Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119 (4 May 2016)

[2] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119 (4 May 2016)

Under this legislation, as reinforced by the jurisprudence of the Court of Justice of the EU (CJEU), the European Commission may grant adequacy status where a third country has data protection standards that are "essentially equivalent" to those of the EU.

European Commission adequacy decisions require sign-off by the EU Member States. The European Data Protection Board (EDPB) must provide the European Commission with its formal opinion on each proposed adequacy decision. The EDPB comprises the heads of one data protection supervisory authority from each EU Member State plus the head of the European Data Protection Supervisor, the EU administrative body supporting the system.

As of September 2024, the European Commission has issued adequacy decisions for 15 jurisdictions: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Isle of Man, Israel, Japan (organisations falling under the Act on the Protection of Personal Information and subject to the Supplementary Rules), Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom, United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay.[3] In May 2024 it was announced that formal adequacy discussions had been opened between the European Commission and Kenya.[4]

What is the UK's post-Brexit data protection regime?

When the UK left the EU, it kept the GDPR as retained EU law, through the European Union Withdrawal Act 2018, supplemented by the Data Protection Act 2018 (both as amended by subsequent secondary legislation).[5] This secondary legislation renamed the retained GDPR as 'UK GDPR'. The UK GDPR includes the power for the UK Government to make its own adequacy decisions, but the UK also took on the European Commission's existing adequacy decisions with respect to third countries, as retained EU law. The secondary legislation also immediately extended UK adequacy status to the EEA.

What are the arrangements for the UK's EU data adequacy?

The UK-EU Trade and Cooperation Agreement (TCA) (Article 782) specified that, for EU data protection purposes, and given the UK's retention of the GDPR, the UK would not count as a third country as long as it did not amend the GDPR, pending the European Commission's adoption of adequacy decisions for the UK.[6]

---

[3] European Commission, 'Adequacy Decisions': https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [accessed 2 October 2024]

[4] Delegation of the European Union to Kenya, 'Kenya and the EU launch very first Adequacy Dialogue on the African continent': https://www.eeas.europa.eu/delegations/kenya/data-protection-kenya-and-eu-launch-very-first-adequacy-dialogue-african-continent_en?s=352 [accessed 2 October 2024]

[5] The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419)

[6] Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, OJ L 149 (30 April 2021). For further background to post-Brexit UK-EU data protection arrangements, see, by our predecessor Committee: European Union Committee, *Brexit: the EU data protection package* (3rd Report, Session 2017-19, HL Paper 7), *Beyond Brexit: trade in services* (23rd Report, Session 2019-21, HL Paper 248), and, with respect to law enforcement, *Beyond Brexit: policing, law enforcement and security* (25th Report, Session 2019-21, HL Paper 250).

The European Commission adopted adequacy decisions for the UK on 28 June 2021 — one each under the GDPR[7] and the LED.[8] The two decisions are legally distinct from each other and adopted under separate processes.

The UK is the only third country to have EU adequacy status under the LED.

Both of the EU's adequacy decisions for the UK expire after four years. These are the only EU adequacy decisions to be sunsetted (other EU adequacy decisions are subject only to a review, at least every four years). The Commission said that it was appropriate to sunset its decisions on the UK given that, after the end of the post-Brexit transitional arrangements, the UK would "administer, apply and enforce a new data protection regime compared to the one in place when it was bound by EU law" and that this might "notably involve amendments or changes to the data protection framework assessed" in the decisions, "as well as other relevant developments".[9] Both of the UK adequacy decisions provide that they may be extended beyond their initial expiry date.

What is the Global Cross-Border Privacy Rules (CBPR) system?

The CBPR system is a voluntary government-backed data privacy certification programme intended to enable international data flows while allowing organisations to show that they meet data protection standards. Countries can become members of the system by signing up to a set of data protection principles and rules. Companies and organisations in member countries can then apply for, and receive, certification as being compliant.

The CBPR system began as an initiative within the Asia-Pacific Economic Cooperation (APEC) group. However, in 2022 the Global CBPR Forum was established, which is open to non-APEC countries. The Forum also allows associate member status.

The full members of the Global CBPR Forum are Australia, Canada, Japan, the Republic of Korea, Mexico, the Philippines, Singapore, Taiwan[10] and the US.

The UK became the first associate member of the CBPR Forum in 2023.[11] In August 2024, Bermuda, the Dubai International Financial Centre, and Mauritius also gained associate status.[12]

---

[7] Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, OJ L 360 (11 October 2021)

[8] Commission Implementing Decision (EU) 2021/1773 of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, OJ L 360 (11 October 2021)

[9] Commission Implementing Decision (EU) 2021/1772, paragraph 288; Commission Implementing Decision (EU) 2021/1773, paragraph 172

[10] Participating as Chinese Taipei

[11] Department for Science, Innovation and Technology, Press Release: *UK gets new status in global data privacy certification programme* on 6 July 2023: https://www.gov.uk/government/news/uk-gets-new-status-in-global-data-privacy-certification-programme [accessed 10 October 2024]

[12] Global CBPR Forum, 'Members and Associates': https://www.globalcbpr.org/about/membership [accessed 2 October 2024]

APPENDIX B: SUMMARY OF EVIDENCE

The UK-EU data adequacy regime since 2021: Should the UK seek to retain EU adequacy status?

Expected consequences if the UK were to lose EU adequacy status.

1. The previous Government pointed out that the UK had granted adequacy status to the EU, so if the UK lost its adequacy status from the EU — covering transfers from the EU to the UK — the free flow of personal data in the other direction "would not be automatically suspended".[13] However, our evidence underlined that the value of the current UK-EU adequacy arrangement lies precisely in the fact that it enables two-way data flows. For example, Joe Jones of the International Association of Privacy Professionals said that it is the "bilateral combination of the arrangements that is so important to organisations on both sides of the channel and the Irish Sea".[14]

2. All our witnesses except one said that the consequences of the UK losing EU adequacy status would be negative. Overall, witnesses said that losing adequacy would increase friction, complexity, uncertainty and thus costs in trade and other interactions between the UK and EU, which would probably feed through into higher prices for consumers;[15] and that losing adequacy would probably also reduce innovation and consumer choice, hurt consumer confidence, and damage the reputation and attractiveness of the UK and UK institutions, as potential destinations for international investment and collaboration.[16] It would also require new activity of the Information Commissioner's Office (ICO), to help organisations navigate a new no-adequacy environment (for example, assisting businesses to put new standard contractual clauses in place).[17]

3. Lori Baker, Director of Data Protection at the Dubai International Financial Centre Authority, was the only witness who said that losing adequacy might be "not necessarily to the UK's disadvantage", at least after an initial period. She suggested that "there are many companies and privacy professionals looking for a new approach to data protection regulation and the UK may be the right country to provide it".[18]

4. In terms of the cost of losing adequacy, the lawyer Eleonor Duhs, the not-for-profit technology organisation Reset, the NHS Confederation and Understanding Patient Data (in a joint submission) and Dr Karen Mc Cullagh, Associate Professor of Law at the University of East Anglia, all cited a study by the New Economics Foundation and the UCL European Institute from 2020, before the European Commission's original adequacy decisions for the UK, which had estimated that failing to secure adequacy status would impose additional compliance costs on UK businesses of £1.0-1.6 billion.[19] Asked about the possible costs to the economy of losing adequacy now, the Information Commissioner, John Edwards, told us that he had seen a range of estimates but that the cost would be "enormous".[20]

5. Witnesses including the Information Commissioner,[21] the Advertising Association, the Market Research Society, and the International Regulatory Strategy Group[22] said that any loss of adequacy status would be particularly difficult for small and medium-sized companies (SMEs), because they had less capacity to operate the alternative mechanisms that would be required.

6. We heard specific examples of the way in which losing adequacy status could cause problems across a wide range of sectors — from UK-based data-processing,[23] international payments systems,[24] cross-border family law cases,[25] and international efforts against money-laundering and cybercrime,[26] to medical[27] and other research,[28] medical treatment (in the NHS and for UK citizens abroad), and NHS international collaborations (including those aiming to raise extra revenue).[29] The NHS Confederation and Understanding Patient Data, in a joint submission, estimated that the cost to the NHS of any loss of adequacy could be in the tens of millions of pounds.[30]

7. The Northern Ireland Human Rights Commission (NIHRC) and Equality Commission for Northern Ireland (ECNI), in a joint submission, and the Armagh-based Centre for Cross Border Studies said that in the context of the Belfast/Good Friday Agreement and the Ireland/Northern Ireland Protocol any loss of adequacy status by the UK would raise difficulties for both North-South and East-West cooperation, at both individual and institutional levels.[31] The NIHRC and ECNI further argued that data protection rights are fundamental rights within the terms of the Belfast/Good Friday Agreement, and that any loss of adequacy by the UK would therefore constitute a violation of the 'no diminution of rights' commitment under Article 2 of the Protocol.

---

[13] Written evidence from HM Government (Department of Science, Innovation and Technology) (DAT0013)
[14] Q 1 (Joe Jones); see also written evidence from the Advertising Association (DAT0010)
[15] Q 54 (Neil Warwick)
[16] For example, Q 57 (Nicola Watkinson)
[17] Q 3 (Joe Jones), Q 32 (John Edwards)
[18] Written evidence from Lori Baker (DAT0022)
[19] Written evidence from Eleonor Duhs (DAT0005), Reset (DAT0006), Dr Karen Mc Cullagh (DAT0008) and the NHS Confederation and Understanding Patient Data (DAT0017); see UCL European Institute and New Economics Foundation: *The Cost of Data Inadequacy* (November 2020): https://www.ucl.ac.uk/european-institute/sites/european_institute/files/ucl_nef_data-inadequacy.pdf [accessed 2 October 2024]
[20] Q 29 (John Edwards)
[21] Q 31(John Edwards)
[22] Written evidence from the International Regulatory Strategy Group (DAT0004), Advertising Association (DAT0010) and Market Research Society (DAT0016)
[23] Written evidence from the Association of British Insurers (DAT0014), UK Finance (DAT0020)
[24] Written evidence from UK Finance (DAT0020)
[25] Written evidence from Eleonor Duhs (DAT0005)
[26] Written evidence from the International Regulatory Strategy Group (DAT0004)
[27] Written evidence from Cancer Research UK (DAT0007), the NHS Confederation and Understanding Patient Data (DAT0017)
[28] The UK Data Service, University of Essex (DAT0012)
[29] Written evidence from the Association of British Insurers (DAT0014), NHS Confederation and Understanding Patient Data (DAT0017)
[30] Written evidence from the NHS Confederation and Understanding Patient Data (DAT0017)
[31] Written evidence from the Centre for Cross Border Studies (DAT0003) and the Northern Ireland Human Rights Commission and Equality Commission for Northern Ireland (DAT0019)

8. With respect to law enforcement cooperation under Part 3 of the UK-EU Trade and Cooperation Agreement (TCA), the former Home Office official Martin Kelly pointed out that the UK having EU adequacy status is not a legal requirement for the operation of Part 3, and that the EU's law enforcement agencies have relationships with counterparts around the world without the home jurisdictions of such international partners having the status. He therefore said that, if the UK were to lose adequacy, continued operation of the law enforcement cooperation tools in Part 3 of the TCA was "technically not impossible". It would, however, be "very difficult".[32] Robert Jones of the National Crime Agency said that his organisation "would be concerned … if anything undermined our ability to exchange data",[33] and Peter Ayling of the National Police Chiefs' Council said that "The seamless transition of data and digital communications must be a high priority, and anything that jeopardises that would be unwelcome".[34]

9. Almost all our witnesses assessed as less satisfactory than adequacy the alternative mechanisms that may be used for international data transfers if no adequacy status is in place. Alternative mechanisms were seen as more complex, more burdensome, more costly and more limited in scope, while also being less robust. The International Regulatory Strategy Group said that, compared to adequacy, "no alternative scenario is available currently to provide equivalent safeguards for consumers, legal certainty and timely access to data for businesses",[35] and the Association of British Insurers said that adequacy was "without question" "the most legally sound and stable way to transfer personal data between the UK and the EU27/EEA".[36] UK Finance said that "putting in place alternative arrangements could involve thousands of contracts to review and amend" and that the process was "likely to cost millions of pounds and take hundreds of hours of time". It also noted that the approvals process for binding corporate rules, to enable international data transfers within multinational companies in the absence of adequacy, has been known to take several years.[37] Zach Meyers of the Centre for European Reform suggested that, in a "worst-case" interpretation, the CJEU's Schrems II decision implied that standard contractual clauses might not be useable at all as an alternative to adequacy, because they cannot address concerns about government access to personal data.[38]

10. With respect to law enforcement cooperation, Robert Jones of the National Crime Agency said that, if the UK lost adequacy status, with respect to organised crime he was "confident that there are channels where [law enforcement agencies] could carry on exchanging information" with EU counterparts, but that there would be a need for "overlapping multiple bilateral arrangements with other partners for them to be able to disseminate data to us", a prospect that he did "not relish … as an operational leader".[39]

11. The UK's are the only EU adequacy decisions which are sunsetted. Paul Sexby, a practising data protection officer, and the not-for-profit technology organisation Reset both suggested that uncertainty over the UK's adequacy status could deter investment.[40] Neil Warwick of the Federation of Small Businesses (FSB) said that the organisation was "really concerned about the whole cliff edge thing again" (although he also assessed as "low" the likelihood of the UK losing adequacy overnight with no knowledge of subsequent arrangements).[41] Joe Jones of the International Association of Privacy Professionals suggested that the Information Commissioner's Office (ICO) might have to divert resources to prepare UK organisations for a potential loss of adequacy.[42]

12. UK Finance said that any loss of adequacy would be especially disruptive if the decision were sudden or unexpected.[43] The Advertising Association and the Data & Marketing Association suggested that the UK might be better-prepared for any loss of adequacy than it once would have been, partly as a result of the Brexit process,[44] but Neil Warwick said that, if possible, the Federation of Small Businesses (FSB) would want a transition period to help its members to adjust.[45] Nicola Watkinson of TheCityUK said similarly that her sector "would need a really long lead time".[46]

13. Several witnesses said that, if the UK were to lose adequacy status, they would expect the UK and European Commission to implement one or several immediate 'workarounds', to avoid the cliff-edge scenario and buy time in which to take steps that would see adequacy restored. As precedents, witnesses pointed to the aftermath of the CJEU's two Schrems rulings against the EU's data protection arrangements with the US.[47] Some witnesses also suggested that, if the Commission had concerns about the UK's data protection regime, it had alternatives to immediately and completely withdrawing its adequacy decisions[48] (although Ruth Boardman of the International Privacy and Data Protection Group suggested that the UK practices that are most likely to raise EU concerns are not sector-specific, which might reduce the scope for solutions that differentiate among sectors or types of data, along the lines of the adequacy arrangement between the EU and Japan).[49]

The value of UK-EU data adequacy

14. The previous Government said that it was working to retain EU adequacy status, because "Maintaining data adequacy between the UK and the EU facilitates the free flow of personal data, keeping compliance costs low for businesses and the public safe in both jurisdictions".[50] The then-Government estimated the value of maintaining adequacy at £410 million in saved compliance costs (with a range of £190-£460 million) and £240 million in retained export revenue (with a range of £210-£420 million). Over ten years, the then-Government put the estimated Net Present Value of continued adequacy at £2 billion (2019 prices, 2020 present value), with the range between £1.6 and £3.4 billion. The Conservative European Forum said that these figures included only direct UK-EU trade, so might underestimate the total

---

[32] Q 49 (Martin Kelly)
[33] Q 64 (Robert Jones)
[34] Q 64 (Peter Ayling)
[35] Written evidence from the International Regulatory Strategy Group (DAT0004)
[36] Written evidence from the Association of British Insurers (DAT0014)
[37] Written evidence from UK Finance (DAT0020)
[38] Q 17 (Zach Meyers); see also Q 74 (Professor Swire)
[39] QQ 64, 70 (Robert Jones)
[40] Written evidence from Paul Sexby (DAT0002), Reset (DAT0006)
[41] QQ 56-57 (Neil Warwick); see also Q 56 (Nicola Watkinson)
[42] Q 3 (Joe Jones)
[43] Written evidence from UK Finance (DAT0020)
[44] Written evidence from the Advertising Association (DAT0010) and Data & Marketing Association (DAT0015)
[45] Q 59 (Neil Warwick)
[46] Q 56 (Nicola Watkinson)
[47] For example, Q 24 (Zach Meyers, Neil Ross)
[48] For example, written evidence from Reset (DAT0006), Open Rights Group (DAT0021)
[49] Q 57 (Ruth Boardman)
[50] Written evidence from HM Government (Department of Science, Innovation and Technology) (DAT0013)

value once supply chain effects are counted in.[51] Dr Karen Mc Cullagh of UEA Law School cited research suggesting that countries with EU adequacy decisions exhibit a 6-14% increase in digital trade.[52]

15. All our witnesses agreed that adequacy was valuable. They said that it reduced administrative burdens and compliance costs, increased legal certainty, and made the UK a more attractive location to invest and do business.[53] Representative organisations described adequacy as "crucial" in financial services[54] and clinical trials,[55] "highly valuable" in advertising,[56] "very important" in data and marketing,[57] "essential" in market research[58] and "fundamental to numerous NHS endeavours",[59] and said that it "significantly benefits" UK research organisations.[60] Dr Karen Mc Cullagh of UEA Law School said that having EU adequacy status also carried a reputational benefit for the UK, and reassured consumers, who "increasingly value high levels of data protection".[61]

16. Witnesses said that adequacy status was valuable partly because of its simplicity and wide scope, compared to the alternatives. The Information Commissioner contrasted the "absolutely seamless and frictionless" nature of adequacy with the "proliferation of instruments" required outside an adequacy framework.[62] Joe Jones of the International Association of Privacy Professionals called adequacy "rather brutal but simple";[63] and the Market Research Society was among witnesses who noted that this simplicity made adequacy especially valuable for small- and medium-sized firms (SMEs).[64]

17. Witnesses pointed to three features of the UK context that heightened the value of EU adequacy: the services-based nature of the UK economy; the UK's strengths and ambitions in science ('science superpower'); and the scale and breadth of the EU-UK relationship. The previous Government said that £161 billion (21%) of UK-EU trade was data-enabled in 2022,[65] and Zach Meyers of the Centre for European Reform told us that around 45% of the UK's ICT exports went to the EU.[66]

18. The Northern Ireland Human Rights Commission (NIHRC) and Equality Commission for Northern Ireland (ECNI), in a joint submission, and the Armagh-based Centre for Cross Border Studies highlighted the particular value of data adequacy in the context of the

[51] Written evidence from the Conservative European Forum (DAT0018)
[52] Written evidence from Dr Karen Mc Cullagh (DAT0008)
[53] For example, Q 17 (Bojana Bellamy), Q 50 (Nicola Watkinson, Ruth Boardman)
[54] Written evidence from the International Regulatory Strategy Group (DAT0004)
[55] Written evidence from Cancer Research UK (DAT0007)
[56] Written evidence from the Advertising Association (DAT0010)
[57] Written evidence from the Data & Marketing Association (DAT0015)
[58] Written evidence from the Market Research Society (DAT0016)
[59] Written evidence from the NHS Confederation and Understanding Patient Data (DAT0017)
[60] Written evidence from The UK Data Service, University of Essex (DAT0012)
[61] Written evidence from Dr Karen Mc Cullagh (DAT0008)
[62] Q 29 (John Edwards)
[63] Q 1 (Joe Jones)
[64] Written evidence from the Market Research Society (DAT0016)
[65] Written evidence from HM Government (Department of Science, Innovation and Technology) (DAT0013)
[66] Q 17 (Zach Meyers)

Belfast/Good Friday Agreement, in facilitating both North-South and East-West cooperation.[67]

19. With respect to law enforcement cooperation, Peter Ayling of the National Police Chiefs' Council said that adequacy was "enormously beneficial" in transitioning to the use of the tools under Part 3 of the Trade and Cooperation Agreement (TCA).[68] For the National Crime Agency, Robert Jones said that his organisation "would obviously want to do everything we can to preserve the current arrangements".[69]

20. Lori Baker, Director of Data Protection at the Dubai International Financial Centre Authority, was the only witness to raise doubts about the long-term value of EU adequacy for the UK. She pointed out that it enables data transfers only from the EU to the UK and, in effect, from the UK to those other jurisdictions that have EU adequacy status. This leaves data transfers between the UK and the rest of the world uncovered. However, within the UK-EU context, even Ms Baker said that adequacy was "an important mechanism for the free-flow of data … [which] provides certainty to businesses sharing data between both jurisdictions".[70]

The operation of the UK's current data protection and data-sharing arrangements

21. Our witnesses largely welcomed the retention of the EU GDPR in UK law after Brexit. This not only facilitated the receipt of EU adequacy status but also allowed the uninterrupted continuation of data flows and existing data protection processes, and entailed a continued commitment to high data protection standards.[71]

22. However, witnesses also identified a number of shortcomings in the UK GDPR and the way in which it is being interpreted and implemented. Cancer Research UK referred to problems in the field of clinical research.[72] The Advertising Association, Data & Marketing Association and Market Research Society all said that organisations in the UK tended to over-rely on consent as a basis for processing and to make too little use of the other — sometimes more straightforward — permissible bases for processing data;[73] Bojana Bellamy, President of the Centre for Informational Policy Leadership at Andrews Kurth LLP, referred to "consent fatigue".[74] Ruth Boardman of the International Privacy and Data Protection Group said that some requirements were overly bureaucratic and that employees sometimes turned their right to make subject access requests into a means of pressuring their employers, concluding that this part of the GDPR "does not work well".[75] Eleonor Duhs was concerned that the great complexity of the GDPR regime was such as to raise rule of law concerns.[76]

---

[67] Written evidence from the Centre for Cross Border Studies (DAT0003) and the Northern Ireland Human Rights Commission and Equality Commission for Northern Ireland (DAT0019)
[68] Q 64 (Peter Ayling)
[69] Q 64 (Robert Jones)
[70] Written evidence from Lori Baker (DAT0022)
[71] For example, written evidence from Reset (DAT0006), Market Research Society (DAT0016), Northern Ireland Human Rights Commission and the Equality Commission for Northern Ireland (DAT0019)
[72] Written evidence from Cancer Research UK (DAT0007)
[73] Written evidence from the Advertising Association (DAT0010), Data & Marketing Association (DAT0015) and Market Research Society (DAT0016)
[74] Q 18 (Bojana Bellamy)
[75] QQ 50, 52 (Ruth Boardman)
[76] Q 1 (Eleonor Duhs) and written evidence from Eleonor Duhs (DAT0005)

23. Witnesses also said that the costs of GDPR were "significant" and "huge".[77] Dr Karen Mc Cullagh of UEA Law School and the lawyer Eleonor Duhs both cited academic research which estimated that the GDPR led to an 8.1% fall in profits across all sectors and a 2.1% fall in profits in the ICT sector, with smaller ICT firms suffering more of a profit loss than larger ones.[78] However, Dr Mc Cullagh cautioned that some of the costs might be one-off, and both she and Bojana Bellamy of the Centre for Informational Policy Leadership suggested that such figures did not capture the potential gains from GDPR in terms of firm reputation and customer satisfaction.[79] Several witnesses said that the costs of GDPR hit small- and medium-sized firms (SMEs) particularly hard; Neil Warwick of the Federation of Small Businesses (FSB) called GDPR "a huge mountain to climb" and indicated that it was still causing compliance concerns for FSB members.[80]

24. With respect to law enforcement cooperation under Part 3 of the TCA, Dr Nora Ni Loideain, Director of the Information Law and Policy Centre at the Institute of Advanced Legal Studies, University of London, noted that it is difficult so far to assess the operation of the new regime, given how recently it came into being. She also noted a lack of oversight of relevant processes, and a gap in statistics on data exchanges for law enforcement purposes.[81] Our witnesses from law enforcement agencies made clear that law enforcement cooperation was more difficult than it had been pre-Brexit, in particular with respect to the UK's loss of access to the Schengen Information System (SIS II) database. However, they also detailed ways in which their organisations had worked, and were continuing to work, to mitigate the difficulties. Robert Jones of the National Crime Agency said that the new arrangements for UK access to the Prüm system were "very successful", and, with respect to the alternatives to SIS II, Peter Ayling of the National Police Chiefs' Council said that "a suboptimal system has been made considerably better over time".[82]

Risks to the UK's adequacy status

25. Our evidence made clear that the institutional set-up of the EU, and the sunsetted nature of the European Commission's current adequacy decisions for the UK, mean that the continuation of the UK's adequacy status faces two distinct potential hurdles: the Commission's renewal decisions by June 2025; and a potential case at, and then negative ruling by, the Court of the Justice of the EU (CJEU), against a Commission adequacy decision for the UK. A CJEU case could potentially be brought against the Commission's past (2021) or prospective future adequacy decisions for the UK, and separately against the Commission's decisions under either the GDPR or the LED.

26. Witnesses pointed out that considerable evidence was available about the approaches that the Commission and CJEU were likely to take to their decisions (or potential decisions) on the UK and about the factors that they were likely to take into consideration. This evidence can be found in the relevant legislation; past Commission assessments and decisions

---

[77] Q 20 (Bojana Bellamy); written evidence from the Advertising Association (DAT0010) and Data & Marketing Association (DAT0015)
[78] Written evidence from Eleonor Duhs (DAT0005) and Dr Karen Mc Cullagh (DAT0008)
[79] Q 20 (Bojana Bellamy); written evidence from Dr Karen Mc Cullagh (DAT0008)
[80] Q 50 (Neil Warwick)
[81] Q 35 (Nora Ni Loideain)
[82] QQ 62-63 and Q 65 (Robert Jones and Peter Ayling)

(including on the UK in 2021); past advisory opinions of the European Data Protection Board; and the jurisprudence of the CJEU.

European Commission renewal decisions in 2025

27. The UK is the only third country to have the GDPR as its legal 'starting point' with respect to data protection. There was a difference of views among our witnesses as to whether this gives the UK more, or less, scope to operate a regime that differs from GDPR:

    - Professor Elaine Fahey, Professor of Law and Humanities at City, University of London, and Dr Elif Mendos Kuşkonmaz, Lecturer in Law, University of Essex (in a joint submission) and the not-for-profit technology organisation Reset, argued that the fact that the UK started with the same legislation as the EU made any divergence easier to spot and potentially more likely to be seen as significant.[83] On this view, third countries that started with very different data protection approaches and regimes had more scope to diverge from EU law and practice.
    - The previous Government and Lori Baker of the Dubai International Financial Centre Authority argued, on the contrary, that, even if the UK did amend its law so that it started to diverge from the GDPR, its legislation would still be far closer to that of the EU than any other third country, including third countries which had EU adequacy status.[84] Given this situation, Ms Baker suggested that, for the Commission to withdraw adequacy status from the UK, while maintaining it with other third countries, would lack credibility and threaten to cast doubt on the supposedly evidenced-based nature of the whole EU adequacy system.[85] Eleonor Duhs agreed that "if the UK's data adequacy doesn't continue then the bar for adequacy will be set impossibly high".[86]

28. The adequacy decisions for the UK are the only EU adequacy decisions which are sunsetted. The Commission's decisions on the UK in 2025 will therefore be the first in which it must decide whether to renew adequacy status, as opposed to awarding it in the first place. There was some discussion among our witnesses as to whether this might make the Commission's past practice a less reliable guide to its likely approach to the UK process in 2025 than would otherwise be the case. The previous Government suggested that the Commission might consider only developments since its (the Commission's) previous decisions on the UK, in 2021, "rather than starting from scratch".[87] The then-Government noted that the Commission had taken this approach in its recent joint review of other countries with adequacy status.[88] Joe Jones of the International Association of Privacy Professionals agreed that post-2021 developments were the Commission's most likely focus.[89]

---

[83] Written evidence from Reset (DAT0006), Professor Elaine Fahey and Dr Elif Mendos Kuşkonmaz (DAT0011)

[84] Written evidence from HM Government (Department of Science, Innovation and Technology) (DAT0013), Lori Baker (DAT0022)

[85] Written evidence from Lori Baker (DAT0022)

[86] Q 4 (Eleonor Duhs)

[87] Written evidence from HM Government (Department of Science, Innovation and Technology) (DAT0013)

[88] Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC, COM/2024/7 final (15 January 2024)

[89] Q 4 (Joe Jones)

29. The fact that the Commission's 2025 decisions will be on renewal, rather than on an initial awarding of adequacy, was one of the factors that witnesses cited in arguing that the decisions were likely to be positive for the UK. Dr Karen Mc Cullagh of UEA Law School argued that the bar for securing renewal was lower than for securing the status in the first place.[90] Several witnesses pointed out that, while the Commission had turned countries down for adequacy status, it had never withdrawn it once granted.

30. In theory, the European Commission's adequacy decisions are technical ones, in which a third country's data protection regime is assessed, on the basis of evidence, against criteria set out in law. However, among witnesses who addressed the issue, there was a large degree of consensus that, in practice, the Commission would also give significant weight to wider political and economic factors. For example, Dr Karen Mc Cullagh of UEA Law School, who has conducted extensive research on the Commission's adequacy decision-making, told us that the Commission gives the "actual or potential trading relationship" between the EU and a third country "equal if not greater weight" in its determinations.[91] Witnesses also referred to the Commission's strategic objectives with respect to a third country, and the general state of the EU's relationship with it. From his distinct perspective, the Information Commissioner said that if there were a risk to the UK's adequacy status, "it is a risk based on political machinations, rather than on principled analysis".[92]

31. The partly pragmatic nature of the Commission's adequacy decision-making was a further factor that led our witnesses largely to think that a positive renewal decision for the UK in 2025 was the more likely outcome. For example, Dr Karen Mc Cullagh of UEA Law School said that the Commission "will not want to jeopardise [the trade relationship] given the economic value of bidirectional personal data flows between the EU and UK".[93] The Conservative European Forum said that "there is strong support for the adequacy decisions within the European Commission",[94] and the lawyer Eleonor Duhs said that the Commission "will do everything it can" to maintain the UK's status.[95] The likelihood of the UK losing adequacy status was assessed as "non-negligible" by UK Finance,[96] but "moderate" by Professor Fahey and Dr Kuşkonmaz,[97] "quite low" by Neil Ross of techUK[98] and "low" by Dr Mc Cullagh and the Data & Marketing Association.[99] The International Regulatory Strategy Group saw the UK's status as being under "no immediate threat",[100] and Zach Meyers of the Centre for European Reform said that the political considerations

---

[90] Written evidence from Dr Karen Mc Cullagh (DAT0008)

[91] Written evidence from Dr Karen Mc Cullagh (DAT0008); see also Q 4 (Eleonor Duhs), Q 17 (Bojana Bellamy, Zach Meyers), Q 22 (Zach Meyers)

[92] Q 30 (John Edwards)

[93] Written evidence from Dr Karen Mc Cullagh (DAT0008)

[94] Written evidence from the Conservative European Forum (DAT0018)

[95] Written evidence from Eleonor Duhs (DAT0005)

[96] Written evidence from UK Finance (DAT0020)

[97] Written evidence from Professor Elaine Fahey and Dr Elif Mendos Kuşkonmaz (DAT0011)

[98] Q 17 and Q 22 (Neil Ross)

[99] Written evidence from Dr Karen Mc Cullagh (DAT0008), Data & Marketing Association (DAT0015)

[100] Written evidence from the International Regulatory Strategy Group (DAT0004)

in play suggested that "adequacy would not be at risk from the Commission" "unless the UK did something terribly egregious".[101]

Possible ruling by the Court of Justice of the EU

32. There was a large measure of consensus among our witnesses that, of the Commission and the CJEU, the latter is the greater risk to the continuation of the UK's adequacy status. For example, the not-for-profit technology organisation Reset called the CJEU "the more exacting forum" of the two and said that the Court "has in recent years consistently taken a more absolute line than the Commission (and most of the Member States) in defence of fundamental privacy rights".[102] Several witnesses pointed out that, in its two Schrems rulings, the CJEU had struck down previous EU adequacy arrangements with a partner as important as the United States. (The key issue in the strike-down was the risk of disproportionate access — and the nature of oversight of the access — by US national security and law enforcement agencies to personal data held by private entities, and the risk of this including transferred data from the EU.) Professor Peter Swire, Professor of Law and Ethics at Georgia Tech Scheller College of Business, told us that "there is an enormous difference between the position of the Commission and the jurisprudence to date of the Court of Justice … when the Commission says yes, it is not over".[103]

Policies and policy areas of interest and potential concern

33. Witnesses identified a large number of UK policies and practices which they said would or could be of interest and potential concern to the European Commission and/or Court of Justice of the EU (CJEU), as they consider (or potentially consider) the UK's data adequacy status. Our evidence included some detailed technical discussion of these issues, but much of this discussion concerned provisions of the previous Government's Data Protection and Digital Information Bill (DPDI Bill) — which was itself being amended in Parliament during our evidence-taking. We have therefore simply consolidated these issues into a single list below, in order to alert the Government to policy matters where it should proceed with an awareness of their potential relevance to the UK's data adequacy status.

34. The issues which witnesses said would be of interest and potential concern to either or both of the European Commission and Court of Justice as they consider, or potentially consider, decisions about the UK's adequacy status included:

---

[101] Q 22 (Zach Meyers)

[102] Written evidence from Reset (DAT0006)

[103] Q 72 (Peter Swire)

- regulatory standards and divergence from the EU, including on:
    - the rights of, and standards of protection for, data subjects[104] — including the threshold to exercise rights, the accessibility of effective redress, and subjects' rights under the prospective regulation of artificial intelligence (AI),[105] automated decision-making (ADM) and facial recognition;[106]
    - lawful bases for data processing and the ability to designate legitimate interests by secondary legislation made by Ministers;[107]
    - the possibility of ending end-to-end encryption;[108]
    - the retention of passenger name recognition (PNR) records;[109]
    - UK Government access to personal data for national security and law enforcement purposes;[110]
- aspects of the UK's national security regime under the Investigatory Powers Act 2016, including data collection and retention, surveillance powers and practices, and the role of the Investigatory Powers Tribunal (with concerns potentially heightened by aspects of the Investigatory Powers (Amendment) Act 2024);[111]

- potential risks posed by onward transfers of data from the UK to other third countries (including under the UK-US Cloud Agreement) (and including unintentional as well as intentional transfers);[112]

---

[104] Q 45 (Dr Ni Loideain), Q 56 (Neil Warwick); written evidence from the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament (DAT0001), International Regulatory Strategy Group (DAT0004), Eleonor Duhs (DAT0005), Reset (DAT0006), Conservative European Forum (DAT0018), Northern Ireland Human Rights Commission and the Equality Commission for Northern Ireland (DAT0019), UK Finance (DAT0020)

[105] Q 41 (Dr Ni Loideain); written evidence from The UK Data Service, University of Essex (DAT0012), UK Finance (DAT0020)

[106] Q 41 (Dr Ni Loideain); written evidence from Eleonor Duhs (DAT0005), The UK Data Service, University of Essex (DAT0012)

[107] For example, Q 21 (Zach Meyers)

[108] Q 75 (Professor Swire)

[109] Written evidence from the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament (DAT0001); Q 35 (Dr Ni Loideain)

[110] Q 6 (Joe Jones), Q 17 (Zach Meyers), Q 22 (Bojana Bellamy), Q 23 (Neil Ross), Q 72 (Professor Swire)

[111] Q 5 (Joe Jones), Q 17 (Zach Meyers), Q 22 (Bojana Bellamy), Q 23 (Neil Ross), Q 41 (Dr Ni Loideain), Q 72 (Professor Swire); written evidence from the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament (DAT0001), Dr Karen Mc Cullagh (DAT0008), Professor Elaine Fahey and Dr Elif Mendos Kuşkonmaz (DAT0011)

[112] Written evidence from the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament (DAT0001), International Regulatory Strategy Group (DAT0004), Eleonor Duhs (DAT0005), Reset (DAT0006), Professor Elaine Fahey and Dr Elif Mendos Kuşkonmaz (DAT0011), Conservative European Forum (DAT0018), the Northern Ireland Human Rights Commission and the Equality Commission for Northern Ireland (DAT0019), Open Rights Group (DAT0021)

- the independence and effectiveness of the Information Commissioner's Office (ICO);[113]
- the deletion in UK law of the concept of EU fundamental rights and their replacement by references to the European Convention on Human Rights (ECHR), and the ending of the supremacy of EU law;[114]
- any legal cases which provide grounds for concern about UK data protection standards;[115]
- the wider UK legislative and policy landscape in areas relevant to data protection, primarily with respect to human rights, the rule of law, and the UK's obligations under international law — including the UK's stance with respect to the European Convention on Human Rights (ECHR), and its non-ratification so far of the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108+').[116]

The scope for change and legislative reform

35. As noted above, witnesses identified a number of shortcomings in the way in which the UK GDPR is currently operating. In this context, they often welcomed the reform intentions of the previous Government's Data Protection and Digital Information Bill (DPDI Bill). However, it was the DPDI Bill that also raised many of the issues that some witnesses said might be of concern to the EU, to the point of potentially jeopardising the UK's adequacy status.

36. A number of witnesses commended the direction of travel that the Bill had taken during its parliamentary proceedings, through the amendments made to the original text. For example, the Data & Marketing Association said that the "amendments made by the Bill to UK GDPR provide some helpful clarifications and interpretations"[117] and the Advertising Association called the Bill a "step in the right direction".[118] Neil Ross of techUK assessed the DPDI Bill as "quite a carefully calibrated evolution of the data protection regime" and, when he gave evidence in April 2024, described matters as being "in quite a good place".[119] He said that he understood that the previous Government had consulted with the European Commission,[120] and Joe Jones of the International Association of Privacy Professionals said

---

[113] Q 5 (Eleonor Duhs); written evidence from the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament (DAT0001), International Regulatory Strategy Group (DAT0004), Eleonor Duhs (DAT0005), Reset (DAT0006), Advertising Association (DAT0010), The UK Data Service, University of Essex (DAT0012), Association of British Insurers (DAT0014), Market Research Society (DAT0016), the Northern Ireland Human Rights Commission and the Equality Commission for Northern Ireland (DAT0019), UK Finance (DAT0020), Open Rights Group (DAT0021)

[114] Q 5 (Eleonor Duhs); written evidence from Eleonor Duhs (DAT0005)

[115] For example, written evidence from the Data & Marketing Association (DAT0015)

[116] For example, Q 6 (Joe Jones), Q 23 (Bojana Bellamy), Q 43 (Dr Ni Loideain); written evidence from Eleonor Duhs (DAT0005)

[117] Written evidence from the Data & Marketing Association (DAT0015)

[118] Written evidence from the Advertising Association (DAT0010); see also Q 27 (Bojana Bellamy, Zach Meyers), Q 52 (Neil Warwick), Q 56 (Ruth Boardman)

[119] QQ 17-19 and Q 21 (Neil Ross)

[120] Q 17 (Neil Ross)

that his "strong sense is that the reforms have been designed with a view to retaining EU adequacy".[121]

37. More widely, witnesses said that there was scope for the UK to make reforms without necessarily risking its adequacy status. Ruth Boardman of the International Privacy and Data Protection Group said that "there are certainly amendments that can be made that would reduce the burden on business without risking adequacy being lost",[122] and the former Home Office official Martin Kelly said that "It was always accepted, throughout the adequacy discussion process, that over time there would be some divergence. There is no problem with that".[123] Witnesses including Professor Fahey and Dr Kuşkonmaz and the Data & Marketing Association suggested that the main lesson for the UK from the European Commission's recent review of other third countries with adequacy status was that such countries could maintain data protection laws that were quite different from that of the EU, and introduce innovations in their data protection regimes, and still enjoy EU adequacy status.[124]

38. With respect to navigating the EU adequacy regime as a third country, Japan was the country which witnesses cited most often as an example that the UK might usefully follow — more in terms of the 'how' than the 'what', in the words of Josh Lee Kok Thong, Managing Director for Asia-Pacific at the Future of Privacy Forum.[125] The Advertising Association said that the case of Japan "demonstrates how countries can bridge differences through constructive engagement and a willingness to adapt existing frameworks",[126] and the Data & Marketing Association said on the basis of the Japanese case that "maintaining a close relationship [and] being open and transparent about changes made in domestic law and why … give strong pointers about an effective approach".[127]

39. From their different perspectives, and independently of its potential implications for the UK's adequacy status, the lawyer Eleonor Duhs, Cancer Research UK and Neil Ross of techUK all warned against any lowering of data protection standards that might reduce the public's trust and willingness to share their data.[128]

Wider international data protection policy

40. It was clear from our evidence that the potential for onward transfers of EU citizens' data, from an EU-adequate third country to a non-adequate one, is for the EU among the most sensitive of data protection issues. Now that the UK is able to make its own adequacy decisions, Dr Mc Cullagh of UEA Law School said that it must ensure that they "cannot be used as a 'back door' to circumvent GDPR adequacy requirements, particularly in respect of onward transfers", because "Doing so would jeopardise the EU-UK adequacy

---

[121] Q 6 (Joe Jones); see also Q 41 (Martin Kelly)

[122] Q 50 (Ruth Boardman)

[123] Q 43 (Martin Kelly)

[124] Written evidence from Professor Elaine Fahey and Dr Elif Mendos Kuşkonmaz (DAT0011), Data & Marketing Association (DAT0015)

[125] Q 76 (Josh Lee Kok Thong)

[126] Written evidence from the Advertising Association (DAT0010)

[127] Written evidence from the Data & Marketing Association (DAT0015)

[128] Q 21 (Neil Ross); Written evidence from Eleonor Duhs (DAT0005), Cancer Research UK (DAT0007)

decision".[129] Professor Swire confirmed that "there is a tension" between retaining EU adequacy and the UK's actual and potential arrangements of its own with non-EU states.[130] Several witnesses suggested that potential transfers from the UK to non-EU-adequate members of the Global Cross-Border Privacy Rules (CBPR) system would raise EU concerns of this kind. Zach Meyers of the Centre for European Reform noted the exclusion of onward transfers under CBPR from the EU's adequacy decision for Japan.[131]

41. However, witnesses — including the Civil Liberties Committee (LIBE) of the 2019–24 European Parliament — also largely indicated that the UK's current associate status in the Global CBPR Forum, and even potential full participation in the CBPR system, would not necessarily jeopardise its retention of EU adequacy status.[132] Witnesses including the previous Government pointed out that several countries were members of the Forum while also having EU adequacy.[133] Josh Lee Kok Thong of the Future of Privacy Forum was somewhat more cautious, saying that "it was hard to say for sure" what the implications for the UK's adequacy would be of full CBPR membership. He advocated "regular dialogue and review of the arrangement and cooperation with the EU" as a means of addressing any concerns.[134]

42. Our evidence made clear that the future of international data protection arrangements is very much up for current discussion, among policymakers, experts and stakeholders in several parts of the world. Joe Jones of the International Association of Privacy Professionals suggested that there were two broad approaches to the future international environment: one in which the EU adequacy system continues to expand and eventually becomes a global regime; and one featuring new multilateral arrangements.[135]

43. Witnesses differed on the potential for the CBPR system to develop into a wider international data privacy regime. Zach Meyers of the Centre for European Reform tended towards caution, pointing to the low number of firms that had signed up to the system so far and saying that it "has quite a long way to go before it can compete with the GDPR" in terms of the number of firms it covers.[136] Joe Jones of the International Association of Privacy Professionals too said that the GDPR had become "the global model".[137] Other witnesses, such as Bojana Bellamy (Centre for Informational Policy Leadership), Neil Ross (techUK), Professor Swire and the Information Commissioner,[138] warned of the limitations of GDPR and its international expansion, and were more upbeat about the opportunities represented by the CBPR. Professor Swire said that an adequacy system "just does not scale".[139]

---

[129] Written evidence from Dr Karen Mc Cullagh (DAT0008)
[130] Q 79 (Peter Swire)
[131] Q 25 (Zach Meyers); see also Q 14 (Joe Jones)
[132] Written evidence from the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament (DAT0001)
[133] Written evidence from HM Government (Department of Science, Innovation and Technology) (DAT0013)
[134] Q 77 and Q 78 (Josh Lee Kok Thong)
[135] Q 12 (Joe Jones)
[136] Q 25 (Zach Meyers)
[137] Q 1 (Joe Jones)
[138] Q 17 (Bojana Bellamy, Neil Ross), Q 25 (Bojana Bellamy, Neil Ross), Q 34 (John Edwards)
[139] Q 78 (Peter Swire)

44. Josh Lee Kok Thong of the Future of Privacy Forum and Bojana Bellamy of the Centre for Informational Policy Leadership both felt that the UK had a potential role to play in international discussions around future global data protection arrangements.[140] Josh Lee Kok Thong said that the UK was "in a unique position vis-à-vis the adequacy system under the GDPR as well as the CBPR system" and that the country could "potentially position itself as a leader in the conversation on cross-border data transfers globally".[141]

[140] Q 25 (Bojana Bellamy), Q 77 (Josh Lee Kok Thong), Q 78 (Josh Lee Kok Thong)

[141] Q 77 (Josh Lee Kok Thong), Q 78 (Josh Lee Kok Thong)