House of Commons

Exiting the European Union Committee

The progress of the UK's negotiations on EU withdrawal: Data

Seventh Report of Session 2017–19

Report, together with formal minutes relating to the report

Ordered by the House of Commons to be printed 26 June 2018

HC 1317
Published on 3 July 2018
by authority of the House of Commons

Exiting the European Union Committee

The Exiting the European Union Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of the Department for Exiting the European Union and related matters falling within the responsibilities of associated public bodies.

Current membership

Hilary Benn MP (*Labour, Leeds Central*) (Chair)

Mr Peter Bone MP (*Conservative, Wellingborough*)

Joanna Cherry MP (*Scottish National Party, Edinburgh South West*)

Sir Christopher Chope MP (*Conservative, Christchurch*)

Stephen Crabb MP (*Conservative, Preseli Pembrokeshire*)

Mr Jonathan Djanogly MP (*Conservative, Huntingdon*)

Richard Graham MP (*Conservative, Gloucester*)

Peter Grant MP (*Scottish National Party, Glenrothes*)

Wera Hobhouse MP (*Liberal Democrat, Bath*)

Andrea Jenkyns MP (*Conservative, Morley and Outwood*)

Stephen Kinnock MP (*Labour, Aberavon*)

Jeremy Lefroy MP (*Conservative, Stafford*)

Mr Pat McFadden MP (*Labour, Wolverhampton South East*)

Craig Mackinlay MP (*Conservative, South Thanet*)

Seema Malhotra MP (*Labour (Co-op), Feltham and Heston*)

Mr Jacob Rees-Mogg MP (*Conservative, North East Somerset*)

Emma Reynolds MP (*Labour, Wolverhampton North East*)

Stephen Timms MP (*Labour, East Ham*)

Mr John Whittingdale MP (*Conservative, Maldon*)

Hywel Williams MP (*Plaid Cymru, Arfon*)

Sammy Wilson MP (*Democratic Unionist Party, East Antrim*)

Powers

The Committee is one of the departmental select committees; its powers are set out under a Temporary Standing Order of 4 July 2017.

Publication

Committee reports are published on the Committee's website at www.parliament.uk/exeucom and in print by Order of the House.

Evidence relating to this report is published on the inquiry publications page of the Committee's website.

Committee staff

The current staff of the Committee are James Rhys (Committee Clerk), Claire Cozens (Second Clerk), Dr Ariella Huff (Senior Committee Specialist), Shakera Ali (Committee Specialist), Duma Langton (Committee Specialist), Judy Goodall (Committee Specialist), Adrian Hitchins (Committee Specialist), Julian Mazowiecki (Committee Specialist), Eoin Martin (Committee Specialist), Leo Oliveira (Senior Committee Assistant), Pansy Barrett (Senior Committee Assistant), Henry Ayi-Hyde (Committee Assistant), Estelle Currie (Senior Media Officer) and Ben Shave (Media and Communications Officer).

Contacts

All correspondence should be addressed to the Clerk of the Exiting the European Union Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 7568; the Committee's email address is exeucom@parliament.uk.

Contents

Conclusions

Data and the modern world

1. Data flows and data protection are fundamental to the modern way of life and, increasingly, to the functioning of the economy, particularly in areas of UK comparative advantage such as services. The objective in the negotiations for the UK Government must be to maintain high standards of data protection and ensure that data can continue to be transferred across borders as it is now. (Paragraph 7)

EU data protection and third countries

2. The EU's existing arrangements for providing for data flows with third countries typically involve a decision of adequacy from the European Commission. Since the CJEU decision on the US-EU Safe Harbour agreement, a decision of adequacy will require the third country to provide protection of fundamental rights essentially equivalent to that provided in the EU. A range of countries have received an adequacy decision, ranging from Switzerland to Argentina to New Zealand. The United States and Canada have limited arrangements. (Paragraph 16)

The negotiation positions

3. The UK's proposals accept that the EU will need to assess the adequacy of the UK data regime. The UK is asking for this to be on the basis of a two-way agreement—rather than solely a one-way decision of the European Commission—and in the form of an international agreement—a Treaty. The UK should provide more information on the distinction between the procedure for an adequacy decision and the procedure that it expects both parties to go through to secure an international agreement on data. (Paragraph 30)

4. The EU negotiating guidelines on the future relationship provide that data protection should be governed by EU rules on adequacy. The public statements from Michel Barnier have consistently said that the EU will not share its regulatory autonomy with a third country. The UK has said it does not wish to interfere with the EU's decision-making autonomy and respects the fact that certain EU bodies are subject to CJEU jurisdiction. The EU appears to consider the UK proposals to be an attempt to retain influence on the EU regulatory regime from the position of a third country. The UK should accept, to increase the prospects of securing the Prime Minister's objectives of continuing membership by the Information Commissioner on the European Data Protection Board and representation under the European One-stop shop, that the CJEU will continue to have jurisdiction over aspects of data protection law in the UK after exiting the EU. (Paragraph 31)

5. The EU have said as a third country that the UK cannot have continued participation on the European Data Protection Board or One-stop shop. No non-EU states are represented on the European Data Protection Board; and while non-EU EEA countries such as Norway are within the internal market on data they do not participate on the European Data Protection Board. The EU wishes to retain its decision-making autonomy, and the UK may be put in a position where it does not have a role in helping to frame future EU wide rules on data. (Paragraph 36)

6. As things currently stand, UK businesses will be outside the provisions of the new One-stop shop, a coordination mechanism designed to reduce cost and bureaucracy to businesses across the EU. (Paragraph 37)

7. The content of the UK proposal is unprecedented for an EU third country arrangement on data and there are no existing models for third country data exchange covering the degree of data sharing in criminal justice that the UK is seeking. The UK would need an adequacy decision to be able to engage in data sharing for law enforcement purposes. It would also have to accept the jurisdiction of the CJEU. It is not in the interests of the people and governments of Europe for there to be a reduction in cooperation in respect of policing and law enforcement. We urge both sets of negotiators to find a way to secure continued high level cooperation on this incredibly important and sensitive matter. (Paragraph 43)

8. There is a high chance of a legal challenge to any proposed UK-EU data international agreement. A legal challenge could create regulatory gaps and uncertainty for business. (Paragraph 47)

Alternatives to adequacy

9. The UK should accept the provisions in Title 7 of the draft Withdrawal Agreement providing assurance about the future protection of personal data already in the UK at the time of withdrawal. Following the passage of the Data Protection Act, the UK's data protection law will be aligned with EU law on the day the UK leaves the EU. As a result, the UK will be in a very strong position when it seeks a declaration of essentially equivalent data protection. However, it is seeking an unprecedented agreement which will be subject to negotiation. The UK Government should be preparing for the adequacy process and ensuring that there is no risk of a gap in legal provision for transferring data between the UK and the EU after December 2020. This would have serious implications for businesses and consumers on both sides. The UK Government needs to establish with the Commission whether it is possible for the adequacy process to be initiated before the UK leaves the EU and, if so, to initiate the process without delay. It needs to provide concrete assurances that data will be able to flow between the UK and the EU after December 2020 on the same terms as now. Beyond this, the UK should explore the possibility of negotiating a bespoke agreement with the EU allowing much closer cooperation in data protection and data sharing which once achieved could replace the third party arrangements conferred by a simple adequacy decision. (Paragraph 51)

10. The alternative legal processes for enabling data transfers, such as standard contractual clauses, binding corporate rules, codes of conduct, and certification mechanisms, are unsatisfactory substitutes for an agreement that data protection rules in the UK are essentially equivalent to that of the EU. Such alternatives would represent a considerable change from the status quo, would place a bureaucratic burden on individual businesses, a burden which would be prohibitive for many small businesses. (Paragraph 57)

11. While there are signs that the EU is moving to the inclusion of data in trade agreements, the current pattern appears to be for a trade agreement to be negotiated separately and in parallel to the process of an adequacy decision. The process for considering an application for data adequacy is not hampered or delayed by being subject to trade negotiations. (Paragraph 62)

12. The Government should state if its intention is to negotiate a single agreement covering the economic and the security aspects of the relationship, or to separate them into more than one agreement so the data aspect of the security relationship is not subject to the procedure for the economic agreement. (Paragraph 63)

1 Data and the modern world

Influence of data in day to day life

1. Data has been described as the new oil.[1] Data is a fundamental part of modern life. Businesses hold data on their customers and employees, and transfer individuals' personal and sensitive data from one point to another, often via the internet, as a matter of routine. Data is used by business to "manage operations, customise and market services, fulfil orders and communicate in a wide range of ways".[2] As the movement of personal data has become more commonplace, so public concern about what their data is used for has become more prominent. This was summed up by the Information Commissioner, Elizabeth Denham, who told us:

> The point is that, bottom line, UK citizens and UK residents expect the highest level of data protection. Certainly, when we are leaving the European Union, citizens and consumers expect that Parliament is going to retain those values and those high standards in law, so that we can continue to protect our citizens. I certainly hear that every day in my office. I know the deep concerns that UK citizens have had about Cambridge Analytica and Facebook, and they expect that we as the UK regulator take strong action.[3]

Current framework for data protection inside the EU

2. As the UK is a Member State, the processing of personal data in the UK is governed by the EU data protection regime, which protects individuals' privacy and other information rights. This regime permits the transfer of personal data within the European Economic Area (EEA)—28 EU Member States plus Norway, Iceland and Liechtenstein. The Data Protection Act 2018 is the current legal basis for data protection in the UK.[4] The legislation ensures compliance with the General Data Protection Regulation (GDPR) and transposed the Law Enforcement Directive.[5] The GDPR introduced:

- Extra territorial applicability in some areas. Any data controller and data processor in the EU, or someone offering goods and services to data subjects in the EU, will have to adhere to EU standards.
- Financial penalties. Companies which break the EU data protection rules can be subject to considerable fines.
- The European Data Protection Board (EDPB) replaces the Article 29 Committee, comprising representatives of the designated supervisory authority in each EU country, and representatives from the EU institutions and the Commission. The UK Information Commissioner sits on the EDPB.
- The One-stop shop—creating a role of lead data protection authority in a Member State, which would regulate the GDPR in that state. Companies operating in several Member States only have to deal with one regulator.

1 Attributed to Clive Humby, a mathematician, in 2006, see The Guardian, Tech giants may be huge, but nothing matches big data, 23 August 2013; The Economist, The world's most valuable resource is no longer oil, but data, 6 May 2017; Wired, Data Is the New Oil of the Digital Economy, 6 May 2017

2 techUK, UK Finance and Dentons LLP, No Interruptions, November 2017

3 Q1602

4 ICO Data Protection Act 2018

5 EU Data Protection Directive 2016/680

Importance of ensuring data can still flow

3. The ability to move data, while at the same time providing reassurance to the public that their personal data is safe, is increasingly important to business. In its recent document on data protection, the UK Government said that "All trade is increasingly reliant on data flows".[6] The flow of personal data between the EEA and the UK is "fundamental to the EEA's and UK's increasingly digitised, information-driven, economy and society".[7] Cross-border data flows in and out of the UK increased 28-fold between 2005 and 2015 and are expected to grow another five times by 2021. Three-quarters of the UK's cross-border data flows are with EU countries.[8]

4. A joint report from techUK and UK Finance described being able to move personal data as "an integral part of trade and business" and explained that businesses hold and use the personal data of their customers and employees in a range of ways, for internal operations, to market services, to fulfil orders and to communicate. The report pointed out that many such activities involve the transfer of personal data, commonly via the internet, and "such transfers are routine and ubiquitous across the EEA." These data transfers are part of a company's business model and are reflected in the physical infrastructure of the business, such as the location of data centres. These are arrangements that are rarely simple or cost-free to adapt or restructure.[9]

5. The importance of data to business in a modern economy is pronounced in an economy with a reliance on services, such as the UK. A Frontier Economics report on the digital economy said that:

> service industries account for 79 per cent of output and 43 per cent of trade exports across the country. For the digital sectors, those same figures are 96 per cent and 81 per cent. Economists estimate that about half of all trade in services is "digitally enabled"—they have the potential to be delivered remotely via information and communication links.[10]

6. These general themes were reinforced in our evidence sessions with businesses, and not just those operating in the digital economy. Stephen Hurley, Head of Brexit Planning and Policy, BT, said that the impact of Brexit on data flows was "one of our top two or three concerns", affecting both how BT related to its customers, and also its internal human resources and billing systems.[11] Giles Derrington, Head of Policy: Brexit, International and Economics, at techUK, said enabling cross border data flows was seen as "mission critical" for the tech sector, and "absolutely vital" for other sectors.[12] We heard the same messages from a variety of witnesses, such as Glynn Robinson, Managing Director of the IT consultancy firm BJSS, who said "I do not think you can overstate the importance of the data" and that it was important for "pretty much all organisations who are doing a form of commerce at any level.[13] Professor Hannon, Director of Cancer Research in Cambridge,

6 UK Government, Framework for the UK-EU partnership: Data protection, May 2018
7 techUK, UK Finance and Dentons LLP, No Interruptions, November 2017
8 House of Lords EU Committee, Third Report of 2017–19, European Union Committee, Brexit: the EU data protection package, HL 7. See also the UK Government, the exchange and protection of personal data, 24 August 2017
9 techUK, UK Finance and Dentons LLP, No Interruptions, November 2017
10 Frontier Economics, the UK Digital Sectors After Brexit, 24 January 2017
11 Q1562
12 Q1562
13 Q1295

told us about the importance of data for clinical trials, as did Dr Beth Thompson, from the Wellcome Trust.[14] Chris Cummings, from the Asset Management Association, told us that

> We manage some £1.7 trillion-worth of European assets here in the UK; £1.7 trillion, with European clients coming from the EU-27, normally with the legal vehicle, the fund domicile being in Luxembourg or Dublin but the fund management expertise being here in the UK. Therefore, you can see that a three-way relationship means how absolutely essential it is that getting the data adequacy statement sorted out very quickly becomes hugely important for the industry.[15]

7. **Data flows and data protection are fundamental to the modern way of life and, increasingly, to the functioning of the economy, particularly in areas of UK comparative advantage such as services. The objective in the negotiations for the UK Government must be to maintain high standards of data protection and ensure that data can continue to be transferred across borders as it is now.**

14 Q681, Q1713, Q1745. techUK, UK Finance and Dentons LLP, No Interruptions, November 2017

15 Q1357

2 EU data protection and third countries

Data adequacy decision

8. An adequacy assessment is the specific legal process by which the European Commission examines a third country's laws, practices and international commitments, to establish whether it provides a level of protection that is essentially equivalent to that of the EU. This results in the third country being given an adequacy decision. The adoption of an adequacy decision involves

- The third country requesting an adequacy finding or the Commission approaching the third country;
- A review by the European Commission of the third country's legislative framework;
- An assessment by the European Data Protection Board of the data protection of the third country according to GDPR adequacy criteria;
- A declaration of adequacy; and
- Ongoing monitoring by the Commission.

9. If the UK requests a decision of adequacy, it will be assessed under the GDPR criteria. These include an assessment of the data protection law, the degree of independence of the data protection authority, the administration of the law, the activities of national security and intelligence agencies, and whether or not there was protection and redress for EU residents.[16] An adequacy decision must comply with the EU Treaties, the Charter of Fundamental Rights,[17] the GDPR and all corresponding CJEU caselaw. It would be subject to periodic review, at least every four years.[18] The GDPR states that

> The protection of natural persons in relation to the processing of personal data is a fundamental right.

And refers to Article 8(1) of the Charter of Fundamental Rights of the EU.[19] Elizabeth Denham told us that she expected the Commission to scrutinise adequacy decisions more robustly under GDPR.[20]

16 Article 45 GDPR Transfers on the basis of an adequacy decision

17 Article 51 of the Charter of Fundamental Rights states "The provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof according to their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties".

18 Article 45(3)

19 GDPR Recital 1 Data protection as a fundamental right. See also written evidence from the Information Commissioner to the Joint Committee on Human Rights HRB0054

20 Q1570

10. The effect of an adequacy decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary. In other words, transfers to the country in question will be assimilated to intra-EU transmissions of data.[21] Countries which have received data adequacy decisions include: Andorra, Argentina, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay. There are agreements with Canada for commercial organisations, and the Privacy Shield framework for data transfers with the US. James Mullock, Partner, Bird and Bird, said that, to his knowledge, no country had lost a decision of adequacy once it had been awarded.[22]

11. It has been suggested that the UK securing an adequacy decision may be at risk due to the UK Government's intention to not incorporate the EU Charter of Fundamental Rights (specifically Article 8) into UK law, and its national security legislation.[23] While James Mullock said not incorporating the Charter would make it "more difficult" to secure an adequacy decision, Stephen Hurley said "it should not hopefully make a difference in practice" while Elizabeth Denham said it "would have been a good signal". Giles Derrington said that Section 2 of the Data Protection Bill has been a "significant step".[24] Mr Derrington said the Commission would consider this to be a question of fundamental rights and as part of the adequacy process the UK will have:

> to prove that our national security apparatus is secure and that third country transfers are not happening to places not deemed adequate by the EU.[25]

Fredrick Erixon, of the European Centre for International Political Economy (ECIPE), said that while he would be "very surprised if there were no recognition of adequacy of the UK", it is likely that several Governments in the EU will raise concerns about data protection in the UK and "especially the use of mass surveillance techniques".[26]

Lessons from the EU-US Safe Harbour and the Privacy Shield

12. The US and EU Commission agreed the 'Safe Harbour' decision in 2000 to enable personal data to move from the EU to the US. This was challenged in 2013 by an Austrian privacy campaigner called Max Schrems.[27] The CJEU decided the Safe Harbour framework did not provide an adequate level of protection "essentially equivalent" to that assured within the EU, and, in 2015 the CJEU declared the Commission's adequacy decision in respect of Safe Harbour invalid. This meant international transfers under the Safe Harbour framework were unlawful, and led to a period of legal uncertainty over the legal basis for transfers of personal data from the EU to third countries.

21 EU Commission, Adequacy of the protection of personal data in non-EU countries
22 Qq1595–1597
23 Home Affairs Committee, UK-EU security cooperation after Brexit, HC 635, para 94
24 Q1630. Section 2 Data Protection Act 2018 requires "personal data to be processed lawfully and fairly, on the basis of the data subject's consent". Article 8 (2) of the Charter reads "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned".
25 Q1581
26 Qq521–522
27 Max Schrems was an Austrian law student who challenged the transfer of his data to the US by Facebook, which is incorporated in Ireland. The first Schrems case led the CJEU to invalidate the Safe Harbour arrangement.

13. James Mullock said that the *Schrems* challenge did not necessarily lead to data transfers being stopped, but rather companies took a risk in carrying on and hoping they would be "cut some slack" by regulators who recognised the position they were in, as long as they were seen to be "trying to patch the position". This meant putting in place alternative mechanisms, such as model contracts.[28] The EU and the US agreed a new framework for transatlantic data transfers to replace Safe Harbour, called 'Privacy Shield', in 2016.[29]

14. The EU-US Privacy Shield framework became operational on 1 August 2016 and includes:

- strong data protection obligations on companies receiving personal data from the EU,
- safeguards on US government access to data,
- effective protection and redress for individuals, and
- an annual joint review by EU and US to monitor the arrangement.[30]

15. Elizabeth Denham explained that the UK had reviewed the legal framework around security and intelligence-gathering, resulting in a new independent Investigatory Powers Commissioner, and the Government had committed to improve the transparency and accountability of the intelligence services. The ICO took part in the assessment of the Privacy Shield and it can anticipate the likely questions that the UK will be asked.[31]

16. **The EU's existing arrangements for providing for data flows with third countries typically involve a decision of adequacy from the European Commission. Since the CJEU decision on the US-EU Safe Harbour agreement, a decision of adequacy will require the third country to provide protection of fundamental rights essentially equivalent to that provided in the EU. A range of countries have received an adequacy decision, ranging from Switzerland to Argentina to New Zealand. The United States and Canada have limited arrangements.**

28 Qq1578–1579
29 House of Lords EU Committee Report, Third Report of 2017–19, Brexit: the EU Data Protection Package, HL 7
30 European Commission, EU-US Privacy Shield, July 2016
31 Qq1590–1591

3 The negotiation positions

The UK position

17. The Government recognised the importance of data in its January 2017 White Paper,[32] and on 24 August 2017 published a future partnership paper on data which called for a model of exchanging and protecting personal data including:

- regulatory cooperation, including an ongoing role for the ICO to be involved in future EU regulatory dialogue,
- certainty and stability for businesses, and reducing the risks of the basis for data flows to unexpectedly changing,
- that the UK and EU agree "early on in the process to mutually recognise each other's data protection frameworks",
- an extension of current provisions alongside an agreed negotiating timeline for longer-term arrangements,
- ensuring that data can flow between the UK and EU, and also between the UK and third countries with existing EU adequacy decisions.[33]

18. In her Mansion House speech, the Prime Minister listed data protection as the fourth of five foundations that should underpin the future trading relationship, repeated that the UK had "exceptionally high standards of data protection" and emphasised that the UK wanted to "secure an agreement with the EU that provides the stability and confidence for EU and UK business and individuals". She said:

> That is why we will be seeking more than just an adequacy arrangement and want to see an appropriate ongoing role for the UK's Information Commissioner's Office. This will ensure UK businesses are effectively represented under the EU's new 'One-stop shop' mechanism for resolving data protection disputes.[34]

19. On 23 May 2018, the UK Government published a set of slides on data protection. These set out a vision for a deep and special partnership with two core parts: an economic partnership (beyond any existing free trade agreement) and a security partnership. These would "sit alongside cross-cutting areas such as data protection." It recognised that without an agreement on data, there would be risks to trade, consumers and public services, and to citizens' security.[35] The UK proposal said that while the "standard adequacy approach" is an effective way of ensuring a free flow of data from the EU to third countries, it "would not enable national data protection authorities to cooperate as effectively".[36] Therefore, the new model would "build on a statutory adequacy arrangement" and include:

- An appropriate ongoing role for the Information Commissioner on the European Data Protection Board

32 The United Kingdom's exit from, and new partnership with, the European Union, 17 January 2017
33 UK Government, the exchange and protection of personal data, 24 August 2017
34 The Prime Minister's Mansion House speech, 2 March 2018
35 UK Government, Framework for the UK-EU partnership: Data protection, 23 May 2018
36 UK Government, Framework for the UK-EU partnership: Data protection, 23 May 2018, page 15

- Representation under the EU's new One-stop shop,
- Amendment, dispute resolution and termination provisions,
- Provision for the European Commission to conduct an assessment to satisfy itself whether the UK would pass the essentially equivalent test for data protection

It did not refer to the earlier proposal to "mutually recognise" each other's data protection framework, or the request to agree a negotiating timeline for the longer-term arrangements.[37]

20. On 6 June 2018, the UK Government published a Technical Note on the benefits of a new data protection agreement. This repeated the argument that a "legally binding data protection agreement" between the EU and the UK will bring benefits around legal certainty, cooperation on enforcement and investigations, cost savings and efficient processes for EU businesses, and EU regulator access to the ICO's resource and expertise. The paper said:

> These are benefits that a standard Adequacy Decision cannot provide.[38]

Furthermore, it said:

> An agreement will not affect the EU's ability to change its own data protection legislation, nor the EU's decision-making autonomy. The UK is not seeking decision-making power over future EU laws, has no intention to impede EU policy-making in data protection, and respects the fact that certain EU bodies are subject to CJEU jurisdiction.[39]

21. The UK Technical Note said that "a legally binding agreement would give a level of certainty and stability that an Adequacy Decision would not" and referred to the "uncertainty and disrupted data flows" that occurred when the *Schrems* case led to the EU-US Safe Harbour Agreement being struck down. In oral evidence to this Committee, the Secretary of State for Exiting the EU referred to the impact of the *Schrems* arrangements as a measure of how important it was to ensure an agreement on data.[40]

22. The UK Technical Note also drew attention to a Commission Communication, of January 2017, on the exchange of data with third countries, that said

> The Commission will […] develop international cooperation mechanisms with key international partners to facilitate effective enforcement.[41]

37 UK Government, Framework for the UK-EU partnership: Data protection, 23 May 2018, page 17
38 UK Government, Technical note: benefits of a new data protection agreement, 6 June 2018
39 UK Government, Technical note: benefits of a new data protection agreement, 6 June 2018
40 Q1480 Oral evidence taken on the 25 April 2018
41 European Commission, Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal data in Globalised World, 10 January 2017

The EU position

23. The European Council Guidelines for the negotiations on the future UK-EU relationship, published on 23 March 2018, said:

> 14. In the light of the importance of data flows in several components of the future relationship, it should include rules on data. As regards personal data, protection should be governed by Union rules on adequacy with a view to ensuring a level of protection essentially equivalent to that of the Union.[42]

24. On 1 March 2018, in a speech in Brussels, Michel Barnier reiterated that the UK decision to leave the Single Market and the Customs Union, means the UK would leave the EU common supervision and enforcement structures, which would require the UK to make "a number of difficult but necessary choices." He stated that if

> the UK wants to regain its decision-making autonomy. We respect this, as the UK should respect our own decision-making autonomy.

Mr Barnier used the example of personal data to illustrate his point:

> In the Single Market, we have a modern and very detailed regulatory framework that allows for the "free movement" of personal data. This facilitates the collection and exchange of such data. It also provides for supervisory mechanisms, overseen by the Court of Justice of the European Union.
>
> The UK is going to leave this regulatory framework. In the future, the transfer of personal data from the EU to the UK will be subject to strict rules. These rules are designed to protect a fundamental right.
>
> Allow me to be precise on this point. The transfer of personal data to the UK will only be possible if the UK provides adequate safeguards. One example to ensure that adequate safeguards are in place is an "EU adequacy decision". This is an autonomous EU decision. There can be no system of "mutual recognition" of standards when it comes to the exchange and protection of such data.[43]

25. On 26 May 2018, Mr Barnier gave a speech in Lisbon in which he referred to a paper published by the UK earlier that week,[44] which included the proposal for the UK's Information Commissioner to remain on the European Data Protection Board, for the UK to remain in the 'One-stop shop', and that this would be in the interest of EU businesses. He said

> It will especially run counter to the interests of our businesses if we abandon our decision-making autonomy. […] we cannot, and will not, share this decision-making autonomy with a third country, including a former Member State who does not want to be part of the same legal ecosystem as us.

42 European Council Guidelines for the negotiations on the future UK-EU relationship, 23 March 2018
43 Michel Barnier Brussels speech, 1 March 2018
44 UK Government, Framework for the UK-EU partnership: Data protection, 23 May 2018

He asked:

- Who would launch an infringement against the United Kingdom in the case of misapplication of GDPR;
- Who would ensure that the United Kingdom would update its data legislation every time the EU updates GDPR; and
- How the uniform interpretation of the rules on data protection on both sides of the channel would be ensured.[45]

An agreement on data—Treaty

26. The UK proposal is for a legally binding data protection agreement between the EU and the UK, and we heard supportive evidence for this approach. James Mullock said a treaty "is preferable to a decision," and that " a treaty is the ultimate standard to aim for".[46] He added that securing an agreement on data as an international treaty would:

> add a layer of protection in terms of what European courts could do or not do if they felt that the level of adequacy was sufficient or insufficient.[47]

27. Elizabeth Denham also told us that "a bespoke agreement or a treaty is preferable". She said:

> the bespoke agreement or the treaty that is more of a mutual arrangement and not a one-way review is the better option, because, again, the Government have to protect the rights of UK citizens when their data is collected in the EU.[48]

28. This contrasts with an adequacy decision from the Commission, which would be a one-way decision judging whether data protection in the UK was essentially equivalent to that in the EU, and declared adequate according to the Commission, and according to the Council.[49] Stephen Hurley, BT, said that there is a mutual interest in the EU awarding the UK an adequacy decision as

> the flows in data [go] in both directions. I understand from the UK perspective 75% of our data flows are with the EU [and] From a BT perspective there is definitely an interest in having the mutual side of it and I would imagine that is replicated in many businesses across the EU.[50]

45 Michel Barnier Lisbon speech, 26 May 2018
46 Qq1563–1564
47 Q1563
48 Q1592
49 Q1564
50 Q1598

Elizabeth Denham said:

> The point the Government are making and the point that all of the witnesses today are making is that the UK could strive for something more appropriate, which better reflects the integration of our economies and the integration of our security and policing initiatives. That would be a bespoke agreement or a treaty that sits alongside a trade agreement.[51]

29. Giles Derrington said that while the Commission still had the negotiating position that it expected any relationship to be maintained on the basis of an EU adequacy decision, he thought there was "a better understanding at Member State level" of the consequences for their businesses that operate in the UK, if the UK was in a regulatory framework separate from that of the EU. He said

> our assessment is that individual countries are probably more willing to enter into a bigger negotiation than purely adequacy at the moment. […] At the Commission level there is still the idea, "We have an adequacy agreement", and certainly in the current context of negotiation that is where they are.[52]

He hoped that the Commission would shift, for reasons of both business and security. But ultimately, he said:

> the fall-back is just to get an adequacy agreement, because that is the thing that fundamentally breaks data from flowing.[53]

30. **The UK's proposals accept that the EU will need to assess the adequacy of the UK data regime. The UK is asking for this to be on the basis of a two-way agreement—rather than solely a one-way decision of the European Commission—and in the form of an international agreement—a Treaty. The UK should provide more information on the distinction between the procedure for an adequacy decision and the procedure that it expects both parties to go through to secure an international agreement on data.**

31. **The EU negotiating guidelines on the future relationship provide that data protection should be governed by EU rules on adequacy. The public statements from Michel Barnier have consistently said that the EU will not share its regulatory autonomy with a third country. The UK has said it does not wish to interfere with the EU's decision-making autonomy and respects the fact that certain EU bodies are subject to CJEU jurisdiction. The EU appears to consider the UK proposals to be an attempt to retain influence on the EU regulatory regime from the position of a third country. The UK should accept, to increase the prospects of securing the Prime Minister's objectives of continuing membership by the Information Commissioner on the European Data Protection Board and representation under the European One-stop shop, that the CJEU will continue to have jurisdiction over aspects of data protection law in the UK after exiting the EU.**

51 Q1582
52 Q1586
53 Q1578

Regulatory cooperation

The role of the ICO

32. The UK argues that an international agreement on data would allow additional matters to be taken into account beyond those set out by the EU adequacy procedure. It would enable discussion as to the role of the Information Commissioner and the UK's participation in the One-stop shop.[54] Asked whether it would be unprecedented for a regulator from a non-Member State to participate in the European data regulatory forum, Elizabeth Denham said:

> There are ways to be an observer at the European Data Protection Board, but unless a role for the ICO was negotiated through a bespoke agreement or a treaty there is no way in law at present that we could participate in the One-stop shop, which would bring huge advantages to both sides, and also to British businesses.[55]

Article 68 (3) of the GDPR outlines the membership of the European Data Protection Board as being composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives. It does not refer to the EEA Agreement countries of Norway, Iceland or Liechtenstein.[56]

33. Stephen Hurley, BT, said the ICO had "a strong voice around the table of the European Data Protection Board" and if the UK was outside the One-stop shop mechanism,

> BT itself will have to look elsewhere within the EU for an ICO equivalent, essentially, to have that role and be our lead regulator in the EU, which again is another burden that we frankly want to avoid.[57]

Mr Hurley also raised doubt as to whether the Information Commissioner's role on the European Data Protection Board would continue during transition.[58]

One-stop shop

34. The GDPR introduces the concept of the "One-stop shop", creating a role of lead data protection authority in a Member State, which would regulate the GDPR in that state. The UK Technical Note said of the One-stop shop:

> in the case of a major data breach in the UK affecting EU personal data, the One-stop shop would allow a straightforward process, allowing a much simpler way for EU regulators to work with the ICO. The ICO would provide UK expertise and proximity, and would conduct a fuller, more effective and quicker investigation than an EU regulator could. A standard Adequacy Decision would not deliver this.[59]

54 Q1578, Q1582
55 Q1618
56 Regulation (EU) 2016/679 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 (General Data Protection Regulation)
57 Q1619
58 Q1567. See Article 6(c) and Article 123(5) of the Withdrawal Agreement
59 UK Government, Technical note: benefits of a new data protection agreement, 6 June 2018

35. Elizabeth Denham described continued participation in the One-stop shop as being "really advantageous to business".[60] Giles Derrington said the UK's participation in the One-stop shop would be "necessary for businesses to have true confidence that they will be able to continue and that in the long term the alignment works and can function correctly."[61]

36. **The EU have said that, as a third country, the UK cannot have continued participation on the European Data Protection Board or One-stop shop. No non-EU states are represented on the European Data Protection Board; and while non-EU EEA countries such as Norway are within the internal market on data they do not participate on the European Data Protection Board. The EU wishes to retain its decision-making autonomy, and the UK may be put in a position where it does not have a role in helping to frame future EU wide rules on data.**

37. **As things currently stand, UK businesses will be outside the provisions of the new One-stop shop, a coordination mechanism designed to reduce cost and bureaucracy to businesses across the EU.**

Security cooperation

38. In her Florence speech, the Prime Minister said her proposal for future co-operation in areas of security, law enforcement and criminal justice co-operation "is underpinned by high standards of data protection."[62] And in her Munich Speech, the Prime Minister said:

> People across Europe are safer because of this [practical co-operation, data driven law enforcement and co-operation with EU agencies] co-operation and unique arrangements we have developed between the UK and EU institutions in recent years.[63]

In its partnership paper on Data protection, the UK Government said:

> The EU and UK need to continue to cooperate on the secure and timely exchange of personal data between law enforcement agencies to protect our citizens.

39. The UK has opted in to several EU wide data sharing mechanisms, such as the Schengen Information System II (SIS II) which issues alerts for missing and wanted individuals, the Prüm arrangements allowing for checking databases on DNA, fingerprints and vehicle registrations, and the European Criminal Records Information Service (ECRIS) which enables data on criminal convictions to be exchanged.[64] The UK future partnership paper on security, law enforcement and criminal justice, referred to the value of systems for real-time, or very rapid, data exchange. It also referred to the value of multilateral cooperation between Europol and Eurojust.[65]

60 Q1582
61 Q1581
62 Prime Minister's, Florence speech, 22 September 2017
63 UK Government, Framework for the UK-EU partnership: Data protection, 23 May 2018
64 UK Government, Framework for the UK-EU partnership: Data protection, May 2018
65 UK Government, Security, law enforcement and criminal justice, future partnership paper, 18 September 2017
See evidence from the National Crime Agency to the Home Affairs Committee PSC0009

40. There are different arrangements for accessing EU wide law enforcement databases. The SIS II database is operational in 26 Member States and four non-EU Schengen countries (Norway, Iceland, Liechtenstein and Switzerland.) ECRIS is only available to EU Member States.[66] Europol can transfer personal data to a third country if there is an adequacy decision or if there is an international agreement between Europol and the third country including adequate safeguards on privacy and fundamental rights.[67] The UK partnership paper on security, law enforcement and criminal justice pointed out that "A number of third countries, including the US and Australia, have agreements with the EU on the protection of PNR" and that two non-EU countries—Norway and Iceland—have agreements to participate in Prum.[68] (We note that both Norway and Iceland are in Schengen.) The EU and the US have an agreement, called the EU-US Umbrella Agreement, which, taking account of the *Schrems* decision, establishes a framework for the protection of personal data and law enforcement. It does not provide for the lawful authority to transfer data from the EU to the US.[69]

41. The UK proposal stated that existing precedents for EU third country data exchange were not the right starting point for the UK-EU partnership. The UK proposal said the ambition should be to construct a model that enables operational capabilities between the UK and the EU and its Member States, and

> is underpinned by shared principles, including a high standard of data protection and the safeguarding of human rights

At the same time, it said the UK will no longer be subject to direct jurisdiction of the CJEU".[70]

42. The Law Enforcement Directive—which the UK has implemented in the Data Protection Act—allows for data to be shared between EU Member States and third countries if they can ensure an adequate level of protection.[71] Data transfer for commercial reasons and law enforcement reasons are not necessarily discrete, so the UK would need an adequacy agreement in addition to any provision in place to exchange data for policing and security reasons.[72]

43. **The content of the UK proposal is unprecedented for an EU third country arrangement on data and there are no existing models for third country data exchange covering the degree of data sharing in criminal justice that the UK is seeking. The UK would need an adequacy decision to be able to engage in data sharing for law enforcement purposes. It would also have to accept the jurisdiction of the CJEU. It is not in the interests of the people and governments of Europe for there to be a reduction in cooperation in respect of policing and law enforcement. We urge both sets of negotiators to find a way to secure continued high level cooperation on this incredibly important and sensitive matter.**

66 Oral evidence to the Home Affairs Committee, 6 December 2016, Q29
67 Europol Regulation (EU) 2016/794 Article 25
68 UK Government, Security, law enforcement and criminal justice, future partnership paper, 18 September 2017
69 Home Affairs Committee, UK-EU security cooperation after Brexit, HC 635
70 UK Government, Security, law enforcement and criminal justice, future partnership paper, 18 September 2017
71 Law Enforcement Directive 2016/680, Chapter V
72 Q1594, Q1570

Legal challenge

44. In 2016, the CJEU ruled that the indiscriminate retention of electronic communications without further safeguards, including independent judicial authorisation, breached EU law, including the Charter.[73] It is possible that there will be continuing concerns about the UK's data retention and bulk powers in the Investigatory Powers Act.[74] In 2017, following a request from the European Parliament, the CJEU found the EU-Canada Passenger Name Record Agreement to not be compliant with EU law, citing the EU Charter on Fundamental Rights, and the bulk transfer of sensitive data.[75] Following a claim by a single individual, the EU-US Safe Harbour framework was declared invalid as it could not prevent the US intelligence agencies accessing personal data transferred from Europe.[76]

45. When asked about the approach of Member States to the UK's investigatory powers legislation, Fredrick Erixon told us that there are several Governments in the EU that will raise concerns about data protection in the UK and "especially the use of mass surveillance techniques." He said that Germany, in particular, has had problems with the UK in a similar fashion that it had with the US at the start of the TTIP negotiations following the NSA spying scandal.[77] He pointed out that if the Member States took the standard for data protection that it wanted to apply to the US, and applied it against other Member States in the EU, then there would be

> complications for data transfer and data portability inside the EU, simply because what the UK, France and some other Governments in Europe have done is pretty much similar to what existed in America.[78]

He said that while European Governments "did not make a strong legal point of that" at the time, but "it may be that they are going to press on this issue now." He pointed out that this could lead to the UK being judged to a higher standard on data protection to receive an adequacy decision than it would have been as a Member State.[79] As a Member State, the UK can rely upon exemptions in the Law Enforcement Directive on national security grounds.[80]

46. In her Mansion House speech, the Prime Minister acknowledged that after the UK has "left the jurisdiction of the ECJ, EU law and the decisions of the ECJ will continue to affect us." And to illustrate the point, said

> For a start, the ECJ determines whether agreements the EU has struck are legal under the EU's own law—as the US found when the ECJ declared the Safe Harbour Framework for data sharing invalid.[81]

73 C698/15. The Court of Appeal applied the CJEU judgment to the issues in proceedings and found section of DRIPA 2014 to be incompatible with EU law.
74 Q1616
75 House of Commons Library, Brexit: implications for national security, 31 March 2017; Home Affairs Committee, UK-EU security cooperation after Brexit, HC 635
76 Computer Weekly, Max Schrems welcomes ECJ ruling that Safe Harbour is invalid, 6 October 2015
77 Q521
78 Q521
79 Q522
80 Home Affairs Committee, UK-EU security cooperation after Brexit, HC 635, para 95, Law Enforcement Directive 2016/680;
81 Prime Minister's speech, Mansion House, 2 March 2018

An EU-UK data agreement could be referred to the CJEU, and there is a risk that this could delay ratification and implementation of the agreement.[82] Giles Derrington, techUK, acknowledged "we would expect there to be a challenge ultimately."[83]

47. **There is a high chance of a legal challenge to any proposed UK-EU data international agreement. A legal challenge could create regulatory gaps and uncertainty for business.**

Timetable and continuity

48. The Government has expressed a willingness to protect data exchanged before the end of the transition period, and it to be "essentially equivalent" to the level of protection in the EU.[84] The various institutions involved in the adequacy process would be assessing the state of UK law "at the point of Brexit".[85] James Mullock of Bird & Bird told us that, based on previous examples, adequacy decisions generally take about two years.[86] The techUK report *No Interruptions* said that "In normal circumstances, [the] adequacy process can take between three to five years" with "the quickest assessment completed in eighteen months" which was for Argentina.[87] James Mullock said the EU-US Privacy Shield decision took about one year.[88]

49. Our witnesses thought the timetable for adequacy could be shortened if the UK carried out preparatory work in advance, such as anticipating the difficult questions that the UK would be asked. Elizabeth Denham said:

> We have a good story to tell when it comes to adequacy, but work could begin before that time, so that the UK is ready to have those more difficult discussions about national security, intelligence services and data. We have seen those discussions play out in the Privacy Shield assessment.[89]

Stephen Hurley, from BT, said that however the Government chose to proceed, for business planning purposes the concern was the risk "of a gap at some point in the process because of the time it takes", and that at the end of transition "there may be some period of months or possibly longer where there is no adequacy decision in place".[90] At a previous evidence session in the City of London, Huw Evans, Director General, of the Association of British Insurers, told the Committee:

> The agreement on the transition allows enough time to negotiate an adequacy agreement that could then come into force at the point the transition period ends. It is vital it does. Nobody knows how you would possibly manage any form of gap. Data transfers are absolutely central to how all our businesses work and how individuals and businesses are served.[91]

82 Qq1610–1611. Home Affairs Committee, UK-EU security cooperation after Brexit, HC 635, para 105 Article 218(11) TFEU 11 states "A Member State, the European Parliament, the Council or the Commission may obtain the opinion of the Court of Justice as to whether an agreement envisaged is compatible with the Treaties. Where the opinion of the Court is adverse, the agreement envisaged may not enter into force unless it is amended or the Treaties are revised."

83 Q1587

84 UK Government, Framework for the UK-EU partnership: Data Protection, 23 May 2018

85 Q1572

86 Qq1570–1571

87 techUK, UK Finance and Dentons LLP, No Interruptions, November 2017

88 Qq1570–1571. See also Oral evidence to the Home Affairs Committee 5 December 2017 Q110

89 Q1572

90 Q1572

91 Q1357

50. The techUK No Interruptions report said:

> there is no provision for the European Commission to determine the adequacy of the UK as a third country while the UK remains a Member State, there is also no clear prohibition on doing so […] Thus there would appear to be arguments allowing an adequacy assessment for the UK to begin now.[92]

51. **The UK should accept the provisions in Title 7 of the draft Withdrawal Agreement providing assurance about the future protection of personal data already in the UK at the time of withdrawal. Following the passage of the Data Protection Act, the UK's data protection law will be aligned with EU law on the day the UK leaves the EU. As a result, the UK will be in a very strong position when it seeks a declaration of essentially equivalent data protection. However, it is seeking an unprecedented agreement which will be subject to negotiation. The UK Government should be preparing for the adequacy process and ensuring that there is no risk of a gap in legal provision for transferring data between the UK and the EU after December 2020. This would have serious implications for businesses and consumers on both sides. The UK Government needs to establish with the Commission whether it is possible for the adequacy process to be initiated before the UK leaves the EU and, if so, to initiate the process without delay. It needs to provide concrete assurances that data will be able to flow between the UK and the EU after December 2020 on the same terms as now. Beyond this, the UK should explore the possibility of negotiating a bespoke agreement with the EU allowing much closer cooperation in data protection and data sharing which once achieved could replace the third party arrangements conferred by a simple adequacy decision.**

92 techUK, UK Finance and Dentons LLP, No Interruptions, November 2017

4 Alternatives to adequacy

52. Outside an agreement where the UK data protection regime is essentially equivalent to that of the EU, organisations that wish to transfer data between the UK and the EU would have to fall back on alternative data transfer mechanisms.[93] These include specific arrangements, such as standard contractual clauses, binding corporate rules, codes of conduct, and certification mechanisms.[94]

53. We asked our witnesses about the drawbacks of the alternatives, should the UK not receive a data adequacy decision. We were told that the bureaucratic burden would be placed on to individual businesses.[95] Elizabeth Denham said:

> If the UK and the EU cannot come to an agreement, then there would have to be reliable mechanisms put in place, but it would be more burdensome than having a bespoke agreement, a treaty or an adequacy finding.[96]

54. Furthermore, Ms Denham pointed out that there is a current legal challenge against standard contractual clauses,[97] which "is probably the mechanism that a lot of particularly small and medium businesses would use in this scenario." If the challenge was successful, and in the absence of an agreement or adequacy decision, she said "We would have to rely on those other transfer mechanisms, which is consent on a transactional basis for the transfer of data. Again, that is a burden on business".[98] Large multinational companies are better placed than small businesses to manage such bureaucratic burdens.[99] Frederick Erixon, ECIPE, told us:

> If you are a big multinational, you are going to find a way to deal with it. It is going to cost you money but you are going to find a way to deal with it. If you are a small company, it is another thing.[100]

55. Mr Mullock described the extent of the burden:

> They required papers to be signed. They require, in the case of standard contractual clauses, an individual agreement to be put in place between a company that is transferring data and the business that receives it. In the case of binding corporate rules, they require a company to implement a policy to GDPR level and to have that approved; that is a very time-consuming process.[101]

93 Q1572
94 European Commission, Notice to Stakeholders. Withdrawal of the UK from the Union and EU Rules in the Field of Data Protection, 9 January 2018; No adequacy decision, no panic - PwC comments on the latest European Commission statement on Brexit and EU Data Protection Law, 10 January 2018
95 Q1574
96 Q1569
97 Facebook Ireland and Schrems C311/18; The European Court of Justice to rule on the validity of standard contractual clauses, Linklaters, 30 May 2016
98 Q1568
99 Q1575–1577
100 Q525
101 Q1574

He said it could take "at least 18 months" for his clients to clear that process, and it would be for any UK business receiving data from Europe to have to put in place such a mechanism to be able to receive data from the EU.[102]

56. Mr Hurley explained that BT would have to identify which of its 18,000+ suppliers, that move data to and from the EU, would require standard contractual clauses to be put in place. The contractual clauses are in a set form, not designed to deal with modern business practice, and quite cumbersome.[103] Giles Derrington gave the example when Safe Harbour collapsed and one very large techUK member company had to put in place two million standard contractual clauses, and he said that the "cost, time and effort that took was very significant".[104]

57. **The alternative legal processes for enabling data transfers, such as standard contractual clauses, binding corporate rules, codes of conduct, and certification mechanisms, are unsatisfactory substitutes for an agreement that data protection rules in the UK are essentially equivalent to that of the EU. Such alternatives would represent a considerable change from the status quo, would place a bureaucratic burden on individual businesses, a burden which would be prohibitive for many small businesses.**

Data in trade agreements

58. There is a clear relationship between trade and data, in terms of cross border portability of data and the ability to be able to market and provide certain services in another country.[105] This is important for the future UK-EU trading relationship but also for future UK trade deals with other countries. Giles Derrington told us that "you cannot open up any market if you cannot have free flow of data."[106] The UK Government has said that, after it leaves the EU, it wishes to ensure data flows between the UK and third countries with existing EU adequacy decisions.[107]

59. The European Commission is considering how to reconcile the two objectives of data protection and facilitating trade. It has drafted "horizontal provisions for cross-border data flows and for personal data protection" to be part of trade agreements with the aim of trying to reduce barriers to trade, such as forced data localisation in a state's territory. However, the proposals have not been discussed by the Council (but published on the Council's website).[108] It is apparent that there are parts of the Commission which consider data to be a matter for trade and parts which consider data protection to be a fundamental right.[109]

60. Recent attempts to include data as part of an EU trade deal have not worked. Giles Derrington of techUK explained that the original draft text of the EU-Mexico agreement had a holding paragraph to include data, but this subsequently dropped from later text. The same thing happened with the EU-Japan trade negotiations,[110] resulting in falling back on

102 Q1574
103 Q1575
104 Q1574
105 Q520
106 Q1588
107 UK Government, the exchange and protection of personal data, 24 August 2017, para 31
108 European Commission letter on cross-border data flows and EU trade agreements, 1 March 2018
109 Q1576
110 Q1585

an adequacy process.[111] When the EU and Japan Economic Partnership Agreement was finalised in December 2017, the European Commission announced that data protection was being dealt with separately. It said that privacy and security of personal data was a fundamental right, "a central factor of consumer trust in the digital economy," and that the EU and Japan would continue to engage on data adequacy talks.[112] The EU has said it is discussing data adequacy with South Korea.[113]

61. David Henig, Director of the UK Trade Policy Project at the European Centre for International Political Economy, said his assumption was that including data in an agreement with the EU:

> will be extremely painful […] because the EU is really not comfortable with sharing data. It is increasingly putting more conditions on it. I have not gone into this in detail. They have not actually published what they are going to be moving towards in trade agreements, but, for example, the plurilateral Trade in Services Agreement is essentially held up over differences in allowing data to flow between the EU and the US. It is something that we will need to do some work on, to make sure that we are in a good place on it.[114]

Elizabeth Denham said it would be preferable for the EU-UK data agreement to be a standalone treaty on data and not part of a trade agreement "because of the fundamental rights element of data protection."[115]

62. **While there are signs that the EU is moving to the inclusion of data in trade agreements, the current pattern appears to be for a trade agreement to be negotiated separately and in parallel to the process of an adequacy decision. The process for considering an application for data adequacy is not hampered or delayed by being subject to trade negotiations.**

63. **The Government should state if its intention is to negotiate a single agreement covering the economic and the security aspects of the relationship, or to separate them into more than one agreement so the data aspect of the security relationship is not subject to the procedure for the economic agreement.**

111 Q1586
112 European Commission, EU and Japan finalise Economic Partnership Agreement, 8 December 2017
113 Press statement by Commissioner Věra Jourová, Mr. Lee Hyo-seong, Chairman of the Korea Communications Commission and Mr. Jeong Hyun-cheol, Vice President of the Korea Internet & Security Agency, Brussels, 20 November 2017
114 Qq1282–1283
115 Q1564, Q1581

Formal minutes

Wednesday 27 June 2018

Members present:

Hilary Benn, in the Chair

Joanna Cherry	Mr Pat McFadden
Stephen Crabb	Craig Mackinlay
Peter Grant	Mr Jacob Rees-Mogg
Jeremy Lefroy	Stephen Timms

Draft Report (*The progress of the UK's negotiations on EU withdrawal: Data*), proposed by the Chair, brought up and read.

Ordered, That the Chair's draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 30 agreed to.

Paragraph 31 read.

Amendment proposed, to leave out "provide more information on how it sees the relationship working without interfering with the EU regulatory regime. This includes the mechanism for dispute resolution and how the UK will stay aligned with evolving EU data protection law—including CJEU caselaw" and insert "accept, to increase the prospects of securing the Prime Minister's objectives of continuing membership by the Information Commissioner of the European Data Protection Board and representation under the European One-stop shop, that the CJEU will continue to have jurisdiction over aspects of data protection law in the UK after exiting the EU."—(*Stephen Timms*)

Question put, That the amendment be made.

The Committee divided.

Ayes, 4	Noes, 3
Joanna Cherry	Stephen Crabb
Peter Grant	Craig Mackinlay
Mr Pat McFadden	Mr Jacob Rees-Mogg
Stephen Timms	

Question accordingly agreed to.

Paragraph agreed to.

Paragraphs 32 to 63 agreed to.

Question put, That the Report be the Seventh Report of the Committee to the House.

The Committee divided.

Ayes, 5	Noes, 2
Joanna Cherry	Craig Mackinlay
Stephen Crabb	Mr Jacob Rees-Mogg
Peter Grant	
Mr Pat McFadden	
Stephen Timms	

Question accordingly agreed to.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available (Standing Order No. 134).

[Adjourned till Wednesday 4 July at 9.00am

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Wednesday 25 October 2017	*Question number*
Rt Hon David Davis MP, Secretary of State, Department for Exiting the European Union	Q1–153

Wednesday 29 November 2017	
Peter Hardwick, Head of Exports, Agriculture and Horticulture Development Board; **James Hookham**, Deputy Chief Executive, Freight Transport Association; **Sian Thomas**, Communications Manager, Fresh Produce Consortium; **Duncan Brock**, CIPS Group Director, Chartered Institute of Procurement and Supply	Q154–188
Jon Thompson, Chief Executive and Permanent Secretary, HM Revenue and Customs; **John Bourne**, Policy Director of Animal and Plant Health, Department for Environment, Food and Rural Affairs; **Richard Everitt**, Chairman, Port of Dover; **Richard Ballantyne**, Chief Executive, British Ports Association	Q189–251

Wednesday 7 December 2017	
Simon York, Director, HMRC Fraud Investigation Service; **Mike O'Grady**, Deputy Head, Organised Crime Operations North, HMRC Fraud Investigation Service; **Deputy Chief Constable Drew Harris**, PSNI; and **Assistant Chief Constable Stephen Martin**, Head of Crime Operations, PSNI	Q252–301

Wednesday 13 December 2017	
Professor Alexander Türk, Professor of Law, King's College London; **John Cassels**, Partner, Competition, Regulatory and Trade Law, Fieldfisher LLP; and **Dr Scott Steedman**, Director of Standards, BSI and Vice President (policy), International Standards Organisation	Q302–324
Katherine Bennett, Senior Vice President, Airbus UK; **Rod Ainsworth**, Director of Regulatory and Legal Strategy, Food Standards Agency; **Angela Hepworth**, Director of Corporate Policy and Regulation, EDF UK; and **Dr Ian Hudson**, Chief Executive, Medicines and Healthcare Products Regulatory Agency	Q325–375

Wednesday 20 December 2017	
Professor Michael Dougan, Professor of European Law and Jean Monnet Chair in EU Law, University of Liverpool; **Professor Anand Menon**, Director, UK in a Changing Europe; **Stephen Booth**, Director of Policy and Research, Open Europe	Q376–454

Wednesday 10 January 2018

Professor Richard Whitman, Head of School, Professor Politics and International Relations, University of Kent; **Fredrik Erixon**, Director, European Centre for International Political Economy; **Dr Stephen Woolcock**, Associate Professor in International Relations, London School of Economics — Q455–545

Wednesday 17 January 2018

Christophe Bondy, Public International Lawyer at Cooley (UK) LLP and former senior counsel to Canada on the CETA negotiations; **Dr Lorand Bartels**, University of Cambridge and Senior Counsel, Linklaters; **William Swords**, President, UK-Canada Chamber of Commerce — Q546–633

Wednesday 18 January 2018

Professor Greg Hannon, Director, Cancer Research UK Cambridge Institute; **Professor Eilís Ferran**, Pro-Vice Chancellor for Institutional International Relations, Cambridge University; **Dr Andy Williams**, Vice President Cambridge Strategy & Operations, AstraZeneca; and **Michael Lawrence**, Business Development Director, Deimos Space UK — Q634–690

Wednesday 24 January 2018

Rt Hon David Davis MP, Secretary of State, Department for Exiting the European Union — Q691–835

Wednesday 31 January 2018

Dmytro Tupchiienko, Data Protection Lawyer, EY, London; **Michael Emerson**, Associate Senior Research Fellow, Centre for European Policy Studies, Brussels; **Dr Tamara Kovziridze**, Co-founder, Reformatics, Tbilisi — Q836–905

Wednesday 6 February 2018

John Springford, Deputy Director, Centre for European Reform; **Professor Clive Church**, Emeritus Professor of European Studies, University of Kent; and **Professor René Schwok**, University of Geneva — Q906–964

Wednesday 7 February 2018

Professor George Yarrow, Chair of the Regulatory Policy Institute, Emeritus Fellow, Hertford College, Oxford, and visiting professor; **Ulf Sverdrup**, Director, Norwegian Institute of International Affairs; and **Professor Alla Pozdnakova**, Law Faculty, University of Oslo — Q965–1022

Professor Carl Baudenbacher, Judge of the EFTA Court — Q1023–1048

Wednesday 21 February 2018

Emanuel Adam, Director of Policy and Trade, BritishAmerican Business; **Dr Peter Holmes**, Reader in Economics, University of Sussex; **Dr Pinar Artiran**, Assistant Professor, Bilgi University, Istanbul; **Sam Lowe**, Research Fellow, Centre for European Reforma — Q1049–1100

Wednesday 27 February 2018

Pascal Lamy, former Director-General, World Trade Organization — Q1101–1162

Tuesday 20 March 2018

Dr Lars Karlsson, President of KGH Border Services, former Director of World Customs Organisation, Deputy Director General of Swedish Customs — Q1163–1197

Wednesday 21 March 2018

David Campbell-Bannerman MEP — Q1198–1240

Jessica Gladstone, Partner, Clifford Chance LLP; **David Henig**, UK Trade Policy Specialist — Q1241–1284

Thursday 22 March 2018

Iona Crawford, Associate, Freshfields Bruckhaus Deringer LLP; **Sally Jones**, Director for International Trade Policy, Deloitte; **Mike Regnier**, Chief Executive, Yorkshire Building Society; and **Glynn Robinson**, Managing Director, BJSS — Q1285–1310

Thursday 19 April 2018

Andrew Bailey, Chief Executive, Financial Conduct Authority, and **Sam Woods**, Deputy Governor Prudential Regulation, Bank of England — Q1311–1339

Huw Evans, Director General, Association of British Insurers, **Chris Cummings**, Chief Executive, the Investment Association, **Stephen Jones**, CEO of UK Finance, and **Nikhil Rathi**, CEO of London Stock Exchange Plc and Director of International Development — Q1340–1377

Thursday 25 April 2018

Rt Hon David Davis MP, Secretary of State, Department for Exiting the European Union — Q1378–1488

Wednesday 2 May 2018

Jill Barrett, Visiting Reader, Queen Mary University Law School; **Sir Jonathan Faull**, former Director General, European Commission; **Agata Gostynska-Jakubowska**, Senior Research Fellow, Centre for European Reform; **Lord Lisvane**, former Clerk, House of Commons — Q1489–1561

Wednesday 9 May 2018

Giles Derrington, Head of Policy: Brexit, International and Economics, techUK; **Elizabeth Denham**, Information Commissioner; **Stephen Hurley**, Head of Brexit Planning and Policy, British Telecom; **James Mullock**, Partner, Bird & Bird — Q1562–1633

Dr Bleddyn Bowen, University of Leicester; **Colin Paynter**, Managing Director, Airbus Defence and Space UK; **Patrick Norris**, Secretary of the European Affairs Group, UK Space — Q1634–1692

Wednesday 16 May 2018

Dr Sarah Main, Executive Director, Campaign for Science and Engineering; **Dr Beth Thompson MBE**, Head of Policy (UK and EU), Wellcome Trust; **Professor Richard Brook OBE**, President, Association for Innovation, Research and Technology Organisations; **Professor Michael Arthur**, Chair, EU Advisory Group, Russell Group — Q1693–1758

Wednesday 23 May 2018

Suella Braverman MP, Parliamentary Under-Secretary of State, Department for Exiting the European Union, and **Mr Robin Walker MP**, Parliamentary Under-Secretary of State, Department for Exiting the European Union — Q1759–1908

Wednesday 6 June 2018

Nicholas Hatton, Co-Chair, the3million; **Anne-Laure Donskoy**, Co-Chair, the3million; **Barbara Drozdowicz**, Chief Executive Officer, East European Resource Centre; **Dr Mary Tilki**, Member and former Chair, Irish in Britain; **Catherine Hennessy**, Trustee, Irish in Britain — Q1909–1954

Fiona Godfrey, Chair, British Immigrants Living in Luxembourg, and Deputy Chair, British in Europe; **Jane Golding**, Co-Chair, British in Germany, and Chair, British in Europe; **Michael Harris**, Chair, EuroCitizens, Spain; **Kalba Meadows**, Founder, Remain in France Together — Q1955–1996

Wednesday 20 June 2018

Guy Verhofstadt MEP, Brexit Co-ordinator and Chair of the Brexit Steering Group, European Parliament — Q1997–2141

Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

NEG numbers are generated by the evidence processing system and so may not be complete.

1 Association of British Insurers (NEG0007)

2 British Retail Consortium (NEG0010)

3 British in Europe (NEG0021)

4 Dickinson, Rob (NEG0013)

5 Finance & Leasing Association (NEG0018)

6 Freight Transport Association (NEG0004)

7 Freshfields Bruckhaus Deringer LLP (NEG0019)

8 Investment Association (NEG0009)

9 London First (NEG0001)

10 London Market Group (NEG0020)

11 Michael Emerson Centre for European Policy Studies (CEPS) (NEG0012)

12 O'Brien, Dr Charlotte (NEG0008)

13 Port of Dover (NEG0005)

14 Professor Dr. iur. Dr. rer. pol. h.c. Carl Baudenbacher (NEG0014)

15 Professor Graham Virgo Pro-Vice-Chancellor University of Cambridge (NEG0017)

16 Professor René Schwok Global Studies Institute University of Geneva (NEG0016)

17 Rail Delivery Group (NEG0003)

18 Stephen Woolcock LSE (NEG0011)

19 TheCityUK (NEG0002)

20 the3million (NEG0022)

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website. The reference number of the Government's response to each Report is printed in brackets after the HC printing number.

Session 2017–19

First Report	European Union (Withdrawal) Bill	HC 373 (HC 771)
Second Report	The progress of the UK's negotiations on EU withdrawal	HC 372 (HC 862)
Third Report	The progress of the UK's negotiations on EU withdrawal: December 2017 to March 2018	HC 884 (HC 1077)
Fourth Report	The future UK-EU relationship	HC 935 (HC 1150)
Fifth Report	The progress of the UK's negotiations on EU withdrawal (March to May 2018)	HC 1060
Sixth Report	Parliamentary approval of the Withdrawal Agreement and the future relationship	HC 1240
First Special Report	European Union (Withdrawal) Bill: Government Response to the Committee's First Report	HC 771
Second Special Report	The progress of the UK's negotiations on EU withdrawal: Government response to the Committee's Second Report	HC 862
Third Special Report	The progress of the UK's negotiations on EU withdrawal (December 2017 to March 2018): Government response to the Committee's Third Report	HC 1077
Fourth Special Report	The future UK-EU relationship: Government Response to the Committee's Fourth Report	HC 1150