HOUSE OF LORDS

European Union Committee

3rd Report of Session 2017–19

Brexit: the EU data protection package

Ordered to be printed 10 July 2017 and published 18 July 2017

Published by the Authority of the House of Lords

HL Paper 7

The European Union Committee

The European Union Committee is appointed each session "to scrutinise documents deposited in the House by a Minister, and other matters related to the European Union".

In practice this means that the Select Committee, along with its Sub-Committees, scrutinises the UK Government's policies and actions in respect to the EU; considers and seeks to influence the development of policies and draft laws proposed by the EU institutions; and more generally represents the House of Lords in its dealings with the EU institutions and other Member States.

The six Sub-Committees are as follows:

Energy and Environment Sub-Committee
External Affairs Sub-Committee
Financial Affairs Sub-Committee
Home Affairs Sub-Committee
Internal Market Sub-Committee
Justice Sub-Committee

Membership

The Members of the European Union Select Committee are:

Baroness Armstrong of Hill Top
Lord Boswell of Aynho (Chairman)
Baroness Brown of Cambridge
Baroness Browning
Lord Crisp
Lord Cromwell
Baroness Falkner of Margravine
Lord Jay of Ewelme
Baroness Kennedy of The Shaws
Earl of Kinnoull
Lord Liddle
Baroness Neville-Rolfe
Lord Selkirk of Douglas
Baroness Suttie
Lord Teverson
Baroness Verma
Lord Whitty
Baroness Wilcox

The Members of the Home Affairs Sub-Committee, which conducted this inquiry, are:

Baroness Browning
Lord Condon
Lord Crisp
Baroness Janke
Lord Jay of Ewelme (Chairman)
Lord Kirkhope of Harrogate
Baroness Massey of Darwen
Lord O'Neill of Clackmannan
Baroness Pinnock
Lord Ribeiro
Lord Soley
Lord Watts

Further information

Publications, press notices, details of membership, forthcoming meeting and other information is available at http://www.parliament.uk/hleu

General information about the House of Lords and its Committees are available at http://www.parliament.uk/business/lords/

Sub-Committee staff

The current staff of the Sub-Committee are Tristan Stubbs (Clerk), Julia Labeta (Clerk until 11 June 2017), Katie Barraclough (Policy Analyst) and Samuel Lomas (Committee Assistant)

Contact details

Contact details for individual Sub-Committees are given on the website. General correspondence should be addressed to the Clerk of the European Union Committee, Committee Office, House of Lords, London, SW1A 0PW. Telephone 020 7219 5791. Email euclords@parliament.uk

Twitter

You can follow the Committee on Twitter: @LordsEUCom

CONTENTS

Evidence is published online at www.parliament.uk/brexit-eu-data-protection-package and available for inspection at the Parliamentary Archives (020 7219 3074).

Q in footnotes refers to a question in oral evidence.

SUMMARY

The Government has said that it wants to maintain unhindered and uninterrupted data flows with the EU post-Brexit. The Government's White Paper on *The United Kingdom's exit from and new partnership with the European Union*, says, for example, that the UK "will seek to maintain the stability of data transfers between the EU, Member States and the UK."

We support this objective, but were struck by the lack of detail on how the Government plans to deliver this outcome. Our analysis suggests that the stakes are high, not least because any post-Brexit arrangement that results in greater friction around data transfers between the UK and the EU could present a non-tariff trade barrier, putting the UK at a competitive disadvantage. Any impediments to data flows post-Brexit could also hinder police and security cooperation.

The importance of cross-border data flows to the UK cannot be overstated:

- Global Internet traffic across borders increased 18-fold from 2005 to 2012
- Services account for 44% of the UK's total global exports, second only to the US
- Three-quarters of the UK's cross-border data flows are with EU countries

In this report we look at four elements of the EU's data protection package: the General Data Protection Regulation (GDPR), the Police and Criminal Justice Directive (PCJ), the EU-US Privacy Shield and the EU-US Umbrella Agreement. Both the GDPR and the PCJ will enter into force in May 2018 while the UK is still a member of the EU. The EU-US Privacy Shield and EU-US Umbrella Agreement are already in force but will cease to apply to the UK post-Brexit.

For third countries looking to exchange data with the EU, the GDPR and PCJ provide for two broad options. The first would be for the UK to receive an 'adequacy decision' from the European Commission certifying that it provides a standard of protection which is "essentially equivalent" to EU data protection standards.

The second option would be for individual data controllers and processors to adopt their own safeguards offering an adequate level of protection to enable personal data to be transferred out of the EU. This would include tools such as Standard Contractual Clauses, and Binding Corporate Rules. We conclude that these would be less effective than an adequacy decision, and we note the legal challenge known as *Schrems II* against Standard Contractual Clauses. Given the potential uncertainty around the alternative measures and the level of integration between the UK and the EU—three quarters of the UK's cross-border data flows are with EU countries—we recommend that the Government should seek adequacy decisions to facilitate future UK-EU data transfers.

Although an adequacy decision would provide the most comprehensive mechanism for the UK to share data with the EU in an unhindered way, such decisions are only taken in respect of third countries, and follow a set procedure.

This poses a legal impediment to having a decision in place at the moment of exit. To ensure uninterrupted flows of data and to avoid a cliff edge, we urge the Government to ensure that transitional arrangements are agreed to cover the interim period. Not having a transitional agreement for data-sharing for law enforcement presents a particular challenge because fall-back alternatives are not apparent, and would need to be negotiated.

The UK could find itself held to a higher standard as a third country than as a Member State. When considering an adequacy decision, the European Commission will look at a third country's data protection framework in the round, including national security legislation. If the UK were to seek an adequacy decision, the UK would no longer be able to rely on the national security exemption in the Treaty on the Functioning of the European Union that is currently engaged when the UK's data retention and surveillance regime is tested before the Court of Justice of the European Union.

Even though the UK will no longer be bound by EU data protection laws post-Brexit, there is no prospect of a clean break. The legal controls placed by the EU on transfers of personal data outside its territory will apply when data is transferred from the EU to the UK. This will necessarily affect UK businesses that handle EU data. If the UK were to obtain an adequacy decision, the way that EU institutions such as the new European Data Protection Board and the Court of Justice of the European Union interpret the EU's data protection laws could have an effect, albeit indirectly, by altering the standards that the UK would need to meet to maintain an adequate level of protection. Maintaining adequacy also means that any future changes in national practice could affect the UK's adequacy status. Even without an adequacy decision, as long as UK data controllers and processers wish to continue to receive personal data from the EU they will need to maintain data protection standards that continue to meet EU requirements for the transfer of personal data outside its territory.

Similarly, as long as the UK wants to continue to receive unhindered data flows from the EU, the UK will be affected by the EU's data protection standards relating to the onward transfer of personal data to third countries. The UK's departure from the EU-US Privacy Shield and the EU-US Umbrella Agreement may require the UK to demonstrate that it has protections in place with the US that ensure the same level of protection as provided for under the two agreements. If the UK were to obtain an adequacy decision, a lax approach to onward transfers of data to third countries would put that adequacy decision at risk.

The UK's future ability to influence EU rules on data protection is in doubt. We conclude that the Government must retain UK influence, starting by seeking to secure a continuing role for the Information Commissioner's Office on the European Data Protection Board. The Government will also need to replace the institutional platforms currently used to exert influence and find a way to work in partnership with the EU to influence the development of data protection standards at both the EU and global level.

Brexit: the EU data protection package

CHAPTER 1: INTRODUCTION

Background

1. The central plank of data protection law in the European Union is the 1995 Data Protection Directive.[1] The Directive was designed to protect personal data stored electronically or in hard copy, but it was adopted in the age of personal computers and dial-up Internet connections in the mid-1990s. In the intervening decades, technology has moved on: both the volume of data stored electronically and cross-border data flows have grown rapidly.

2. Internet traffic across borders increased 18-fold from 2005 to 2012.[2] This trend is consistent with the wide range of routine activities that now require cross-border data flows, from the sharing of personal data on social networking sites like Facebook, to online shopping from companies like Amazon, to cloud-based computing, which allows individuals and businesses to store data remotely and to access it from any location.

3. The ability to move data across borders has also become central to trade. About half of all trade in services is enabled by digital technologies and the associated data flows.[3] The UK is a leading exporter of services globally, second only to the US, with services accounting for 44% of the UK's total global exports.[4] 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.[5]

4. The effectiveness of the EU's data protection regime (and indeed that of other jurisdictions) relies on legal controls over cross-border transfers, to prevent EU rules being circumvented when personal data is transferred to jurisdictions with less stringent regulation. In practice, the application of such controls can present a non-tariff barrier to trade—which also helps to explain why the 1995 Data Protection Directive was adopted under a Single Market legal base.[6] For the same reason, some trade agreements, such as the Trans-Pacific Partnership Agreement (TPP), seek to impose limits on the

---

1 Directive 95/46/EC on the protection of individuals with regard to the protection of personal data and on the free movement of such data (OJ L 281, 23 November 1995, pp 31-50)

2 CISCO Systems, *Cross Border Data Flows, Digital Innovation, and Economic Growth, The Global Information Technology Report 2016* (July 2016): http://www3.weforum.org/docs/GITR2016/WEF_GITR_Chapter1.2_2016.pdf [accessed 11 July 2017]

3 Frontier Economics, *The UK Digital Sectors After Brexit* (January 2017): http://www.frontier-economics.com/documents/2017/01/the-uk-digital-sectors-after-brexit.pdf [accessed 11 July 2017]

4 The USA exported 15.6% of the world's services in 2015, while the UK exported 7.1%. HSBC and Oxford Economics, *Unlocking the growth potential of services trade* (2016), p.6: https://globalconnections.hsbc.com/grid/uploads/trade_in_services.pdf (see footnotes 11 and 12 of Trade in Services report) [accessed 11 July 2017]

5 Frontier Economics, *The UK Digital Sectors After Brexit* (January 2017): http://www.frontier-economics.com/documents/2017/01/the-uk-digital-sectors-after-brexit.pdf [accessed 11 July 2017]

6 Article 100a, Treaty Establishing the European Community (OJ C 224, 31 August 1992, p 32)

restrictions on cross-border data transfers that signatories can provide for in their national laws.[7]

5. Police and judicial cooperation across national borders also relies on cross-border flows of data. Successive UK Governments have chosen to participate in a range of EU platforms and agreements facilitating data-sharing among EU law enforcement agencies, such as the Second Generation Schengen Information System (SIS II), the European Criminal Records Information System (ECRIS) and the Prüm Decisions, as well as the databases maintained by EU agencies such as Europol and Eurojust.[8] Access to the information and intelligence currently sourced through these channels is vital for UK law enforcement, but relies on shared standards of data protection. These have hitherto been set out in a 2008 Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, and in the individual legal instruments enabling and regulating specific areas of cooperation.[9]

What this report is about

6. In this report, we examine the overhaul of the European Union's data protection standards enacted in 2016, including the adoption of new instruments that will replace the 1995 Data Protection Directive and the 2008 Council Framework Decision. These two instruments will come into force in May 2018, while the UK is still a member of the European Union.

7. When the UK leaves the EU, it will cease to be bound by the EU's data protection laws. But there is no prospect of a clean break: the legal controls placed by the EU on transfers of personal data outside its territory will apply when data is transferred from the EU to the UK. Even after an initial transfer has taken place, EU rules may apply when the personal data of EU residents is processed in the UK. And the data protection agreements that the EU has reached with third countries like the US will cease to apply to the UK, raising the issue of whether those agreements can or should be renegotiated independently. Our report therefore considers the implications of the UK's exit from the EU for cross-border data transfers and for UK data protection policy more generally.

8. This report arises from our routine scrutiny of EU legislative proposals, but also forms part of the coordinated series of Brexit-themed inquiries launched by the European Union Committee and its six Sub-Committees following the referendum on 23 June 2016, which aim to shed light on the main issues likely to arise in negotiations on the UK's exit from, and future partnership with, the European Union. It draws on a series of evidence sessions that the Sub-Committee held between 1 February and 15 March. The Sub-Committee was stood down with the dissolution of Parliament in advance of the June

7 See TPP, Article 14.11: https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf [accessed 05 July 2017]. The TPP has been signed but not ratified. The US withdrew from the agreement on 23 January 2017.

8 The UK's participation in EU legislation on Justice and Home Affairs (JHA) is principally governed by Protocols 19 and 21, Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU) (OJ C 326, consolidated version of 26 October 2012, pp 1-390) which allow the UK to opt in (Protocol 21) or opt out (Protocol 19) of JHA and Schengen measures.

9 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350/60, 30 December 2008, pp 60-71). See also our report on *Brexit: UK-EU security and police cooperation* (7th Report, Session 2016–17, HL Paper 77). See for example Chapters III to V of the 2009 Europol Decision.

2017 General Election. These inquiries, though short, are an opportunity to explore and inform wider debate on the major opportunities and risks that Brexit presents to the UK. This report will also have a bearing on any domestic legislative proposals on data protection that the new Government may introduce in the coming session of Parliament in order to implement the GDPR and the PCJ Directive and pave the way for the UK's post-Brexit data protection regime.

9. The reform of the EU's data protection framework is continuing: related measures, such as the draft e-Privacy Regulation and the draft Regulation on processing of personal data by the EU institutions, are currently under negotiation.[10] The scope of our report does not extend to these proposals, which are still under scrutiny by this Committee and by the European Scrutiny Committee in the House of Commons.

10. **We make this report to the House for debate.**

10 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communication), COM(2017) 010 and Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No. 45/2001 and Decision No 1247/2002/EC, COM(2017) 008

CHAPTER 2: THE EU DATA PROTECTION PACKAGE

Background

11. Individuals' right to protection of their personal data is enshrined in Article 8 of the EU's Charter of Fundamental Rights, which became legally binding on the EU institutions and on Member States with the entry into force of the Lisbon Treaty on 1 December 2009. Article 16 of the Treaty on the Functioning of the European Union (TFEU) provides a specific legal basis for adopting data protection rules with regard to the processing of personal data "by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law," and for adopting rules "relating to the free movement of such data."

Box 1: Article 8 of the Charter of Fundamental Rights of the European Union

Article 8: Protection of personal data

Everyone has the right to the protection of personal data concerning him or her.

Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

Compliance with these rules shall be subject to control by an independent authority.

Source: Charter of the Fundamental Rights of the European Union (OJ C 326/391, 26 October 2012, pp 391–407)

12. In January 2012, the European Commission published proposals for a new legislative framework for data protection within the EU—consisting of a draft Regulation to replace the 1995 Data Protection Directive,[11] and a draft Directive to replace the 2008 Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[12] These proposals came to the EU Home Affairs Sub-Committee for examination in the course of our scrutiny of draft EU legislation.

13. After four years of negotiations among Member States and the EU institutions, the proposals for a new General Data Protection Regulation ("GDPR") and a Police and Criminal Justice Directive ("PCJ Directive", also known as the "Law Enforcement Directive") were adopted by the Council of Ministers and the European Parliament in April 2016. They are due to come into effect in EU Member States in May 2018.[13] The Regulation will have

11 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23 November 1995, pp 31–50)

12 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350/60, 30 December 2008, pp 60–71)

13 Regulation 2016/679 EU on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC; and Directive 2016/680 EU on the protection 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 119/1, 4 May 2016, pp 1-88)

direct effect, that is to say it will apply to all EU Member States from May 2018 without requiring transposition into national legislation. The Directive requires transposition into national law. The Government has said it will bring forward legislation in the current parliamentary session in order to amend and repeal provisions in the UK's 1998 Data Protection Act—the Act that transposed the original 1995 Data Protection Directive—as required.[14]

14. The GDPR and the PCJ Directive recast data protection standards within the EU. But in response to events—principally the October 2015 ruling of the Court of Justice of the European Union in the *Schrems* case[15] about the onward transfer of personal data from the EU to the United States under Safe Harbour, and Edward Snowden's revelations about surveillance of personal data by intelligence services in the US and some of their allies—the EU also concluded two new agreements with the United States last year, in order to address concerns about the fate of personal data transferred from the EU to the US.

15. These new agreements are the EU-US Privacy Shield, which provides a new framework for transatlantic data transfers to replace Safe Harbour, and the EU-US Umbrella Agreement, which establishes a framework of data protection principles and safeguards for personal data transferred between the EU and the US for criminal law enforcement purposes. The Commission Implementing Decision on the adequacy of the protection provided by the EU-US Privacy Shield, and the Council Decisions on signature and conclusion of the EU-US Umbrella Agreement, were subject to our routine scrutiny of draft EU legislation, although in both cases the Government's handling of the parliamentary scrutiny process left much to be desired.[16]

16. Upon leaving the EU, the UK will become a 'third country' for the purpose of EU data protection rules, and all four measures—the General Data Protection Regulation, the Police and Criminal Justice Directive, the EU-US Privacy Shield and the EU-US Umbrella Agreement—will cease to apply to the UK. In the remainder of this chapter, we briefly outline the contents of each of the four new measures adopted last year, then turn to the legal implications of Brexit for the UK's data protection arrangements.

The General Data Protection Regulation

17. The General Data Protection Regulation updates the basic rules and principles enshrined in the 1995 Data Protection Directive, which it will supersede. It sets out the responsibilities of individuals and organisations who manage personal data ("controllers") and those who process data on controllers' behalf ("processors"), as well as the rights of individuals whose personal data is held or processed ("data subjects").

18. The scope of the Regulation specifically excludes activities that fall outside the scope of European Union law, such as national security, and it does not extend to the processing of personal data for criminal law enforcement purposes, which will instead be subject to the new Police and Criminal

14 Q 3

15 *Maximillian Schrems v Data Protection Commissioner* (2015) Case C-362/14: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d50b2632c348e6427f9d6cef351e182585.e34KaxiLc3qMb40Rch0SaxyLaNj0?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=520559

16 Q 8, see also European Union Committee, *Report on 2016–17* (1st Report, Session 2017–19, HL Paper 3) paras 82 and 86.

Justice Directive. The handling of personal data by the EU institutions and agencies is also regulated separately, by instruments that are themselves in the process of being recast.[17]

19. The European Commission says that the GDPR "will enable people to better control their personal data", and that "modernised and unified rules will allow businesses to make the most of the opportunities of the Digital Single Market."[18] In the latter respect, the main change is in the nature of the legal instrument, replacing a Directive with a Regulation, and thereby providing for a greater degree of harmonisation across the Member States.

20. The Regulation introduces a broader definition of personal data.[19] It makes clear that personal data includes online identifiers and location data—putting beyond doubt that IP addresses, mobile device IDs and the like are personal data and must be protected as such. It also introduces the concept of pseudonymous data (personal data that has been subjected to technological measures such as encryption so that it no longer directly identifies the individual) and provides definitions of genetic data and biometric data, which are added to the existing categories of 'sensitive' personal data, and subject to more stringent controls.

21. The GDPR includes new provisions on:

- **Extra-territorial applicability**: one of the most controversial aspects of the Regulation when first proposed was the extension in territorial scope. The GDPR will apply to data controllers and processors established within the EU and also to those established outside the EU who offer goods and services to data subjects in the Union or monitor the behaviour of data subjects in the Union. The Commission justified this by arguing that under current rules, "European companies have to adhere to stricter standards than companies established outside the EU but also doing business in our Single Market. With the reform companies based outside of Europe will have to apply the same rules when they offer goods or services on the EU market. This creates a level playing field."[20] The practical effect of the extra-territorial applicability of the GDPR is that even after the UK leaves the EU, the Regulation will continue to apply to UK controllers and processors who process data in a manner that brings them within scope of the Regulation, even if they are not established inside the EU.

---

17 The current Regulation is Regulation 45/2001/EC, which adapted the rules in the original 1995 Data Protection Directive to the EU institutions (OJ L 008, 12 January 2001, pp 1–22). It was supplemented by Decision 1247/2002/EC (OJ L 183, 12 July 2002, pp 1–2). A proposed new Regulation (Council No 5034/17) will repeal and replace both those measures in order to bring the rules governing EU institutions into line with the GDPR and the proposed reform of Directive 2002/58/EC (the so-called "e-Privacy Directive") (OJ L 201, 31 July 2002, pp 37–47).

18 European Commission, 'Agreement on Commission's EU data protection reform will boost Digital Single Market' (IP/15/6321), 15 December 2015: http://europa.eu/rapid/press-release_IP-15-6321_en.htm [accessed 11 July 2017]

19 Article 4 (1) Regulation (EU) 2016/679 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 (General Data Protection Regulation) (OJ L 119/1, 4 May 2016, pp 1–88)

20 European Commission Fact Sheet, 'Questions and Answers - Data Protection Reform', MEMO/15/6385, 21 December 2015: http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm [accessed 11 July 2017]

- **Penalties**: the GDPR introduces heftier financial penalties against controllers or processors who violate data protection rules. Data controllers can face fines of up to the higher of €20 million or 4 per cent of their global annual turnover.

- **'Privacy by design'**: the GDPR stipulates that data protection safeguards must be built into products and services from the earliest stage of development, and seeks to establish privacy-friendly default settings—for example on social networks or mobile apps—as the norm.

- **The 'one-stop shop'**: the GDPR establishes mechanisms to create consistency in the application of data protection law across the EU. In important cross-border cases where several national supervisory authorities are involved, a single supervisory decision will be taken. This principle will allow companies with subsidiaries in several member states to deal with one single supervisory authority in the member state of its main establishment.

- **The European Data Protection Board**: the Regulation creates new powers for national supervisory authorities, and creates a new European Data Protection Board (EDPB). The Board will consist of representatives of all 28 national supervisory authorities and will replace the equivalent body (the Article 29 Committee) created by the 1995 Directive. The EDPB is expected to have a more powerful role than the Committee which preceded it, and perform an adjudicative, rather than advisory function.[21] The range of tasks allocated to the Board is very wide, and its decisions are expected to be highly influential in the development of data protection norms in the future.[22] The overall task of the board is to ensure the consistent application of the Regulation.

- **Data Protection Officers**: all public authorities and those companies that perform certain data processing operations will need to appoint a data protection officer.

22. The Regulation also seeks to enhance the rights of data subjects with new provisions on:

- **Breach Notifications**: the Regulation obliges companies and organisations to notify the national supervisory authority and, in some cases, data subjects, of security breaches involving personal data (such as hacks).

- **Easier access for individuals to their data**: the GDPR introduces a new principle of transparency, intended to ensure that individuals can access more information on how their data is processed, and that such information is provided in a clear and understandable way, including for example in notices addressed to children. The Regulation also seeks to make it easier for individuals to transfer their personal data between service providers (so-called **data portability**).

- **A clarified 'right to be forgotten'**: the Regulation provides that when an individual no longer wants their data processed, and provided that there are no legitimate grounds for retaining it, the data will

21 Written evidence from the UK Information Commissioner (DPP0001)

22 Rosemary Jay, *Guide to the General Data Protection Regulation*, 1st Edition (London: Sweet and Maxwell, 2017)

be deleted. This is not entirely new—a similar remedy is available under the 1995 Directive as interpreted by the CJEU in the case of *Google Spain v AEPD*.[23] We reported on this in July 2014, describing the Commission's proposal in the draft Regulation as "misguided in principle and unworkable in practice." We expressed concern that would mean treating search engines as data controllers and requiring them to remove links to accurate and lawfully available data.[24]

23. The provisions highlighted above are only a sub-set of the provisions to be found in the GDPR—comprehensive overviews and legal commentary are readily available elsewhere.[25]

24. In evidence to our short inquiry, witnesses drew various aspects of the new Regulation to our attention. Ruth Boardman, joint head of the International Privacy and Data Protection Group at Bird & Bird, told us that because the Regulation builds on existing law, "about two-thirds" of the new Regulation "feels very familiar; all the key principles about fairness, transparency, data accuracy and security are there." She highlighted two "key changes", namely that the Regulation "imposes specific obligations on organisations to take certain steps to ensure that they comply by design rather than by accident", and that in a number of areas, the Regulation tries to "tip things in favour of the individual to make it easier for them to enforce their rights."[26]

25. TechUK drew to our attention the "new, much broader definition of what is personal data" in the new Regulation, meaning that "a huge amount of … data will be subject to the GDPR." They warned that "many companies and organisations have not yet fully grasped the broader definition that sits in the GDPR."[27]

26. Despite having registered "serious concerns"[28] about the draft Regulation during negotiations on the text, the Government now regards the GDPR as a "good piece of legislation in and of itself", thanks to "some significant negotiating success during its development."[29] It offers this as one of two reasons why it plans to implement the GDPR "in full."[30]

27. We asked our witnesses about the resource implications of complying with the GDPR. Matt Hancock MP, Minister of State for Digital, assured us that inside Government, "we are fully resourced to deliver the GDPR." Outside Government, the requirements brought in by the new Regulation "are consistent with best practice for handling data anyway." The Minister predicted that:

---

23 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014) Case C-131/12: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=521255

24 European Union Committee, *EU Data Protection law: a 'right to be forgotten'?* (2nd Report, Session 2014–15, HL Paper 40)

25 See for example DLA Piper, 'A guide to the General Data Protection Regulation' (December 2016): https://www.dlapiper.com/en/uk/insights/publications/2016/12/a-guide-to-the-general-data-protection-regulation/ [accessed 11 July 2017]; Bird & Bird, 'Guide to the General Data Protection Regulation' (May 201): https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en [accessed 11 July 2017]; Rosemary Jay, *Guide to the General Data Protection Regulation*, 1st Edition (London: Sweet and Maxwell, 2017)

26 Q 43

27 Q 42

28 Written Statement HCWS126, Session 2015–16

29 Q 1

30 Q 1

> "Companies that handle data appropriately, have good cybersecurity arrangements and respect the privacy of their customers and those whose data they hold should not find this much of a burden, but it will require some companies that do not have best practice to come up to speed."[31]

28. That view was echoed by others. Elizabeth Denham, the Information Commissioner, told us that the impact on businesses "depends on how much work they have done to comply with the current regime." She noted that Parliament passed the Data Protection Act in 1998, and that although the GDPR will introduce higher standards, "they are evolved standards … if a company has not been doing anything for the last 10 years on data protection … the resource implications are going to be larger."[32] Stewart Room, Partner, PricewaterhouseCoopers, Global Cyber Security and Data Protection Legal Services Leader and UK Data Protection Leader, suggested that although there were "significant capital and resource costs" associated with getting ready for the GDPR, "part of the issue to understand is the extent to which organisations will be spending this money to improve themselves to a new standard, or to catch up on things that they should have been doing under the Data Protection Act 1998 and that they have failed to do."[33] For example:

> "Many organisations, in a technical sense, are retaining electronic data that may not be lawful under the UK's current regime. The GDPR causes them to focus on the subject afresh and they discover a data lake that needs to be drained, so that capital cost is incurred. Arguably, they are incurring that capital cost because they have not worked on the Data Protection Act, not because the GDPR is requiring anything new."[34]

29. Mr Room did, however, highlight the position of small to medium enterprises, warning that while large multinationals could procure professional services support to help them understand how things should be done, "that is not necessarily the same for every organisation in the economy." He identified space for a "strong regulator", suggesting that if the regulator could "create guidance, to-do kits and toolkits, it will reduce the resource load on small businesses."[35]

30. Rosemary Jay, Senior Consultant Attorney at Hunton & Williams emphasised that there were some things in the Regulation that "are not catch-up and are going to be new", such as the security breach notification requirement. But she argued that given the importance of cybersecurity, "one might say that it is a resource that businesses should be looking at." She contrasted the security breach notification requirement with other new aspects of the Regulation, such as "the internal record-keeping requirements and some of the details of the notice requirements, which are heavier than one might have liked", and which she considered "more of regret."[36]

31. The Information Commissioner also noted that the GDPR will remove the requirement for data controllers to register their data processing with their national regulator. In the UK, data controllers pay a fee to register, which

---

31 Q 3
32 Q 31
33 Q 16
34 Q 16
35 Q 16
36 Q 16

is used to fund the Information Commissioner's Office. A new mechanism will therefore need to be devised to fund the regulator. Ms Denham told us that "our new fee structure needs to be approved by Parliament, hopefully before 2018, when our notification fees fall off a cliff and we no longer have £22 million in funding."[37]

The Police and Criminal Justice Directive

32. The Police and Criminal Justice Directive updates the basic rules and principles enshrined in the 2008 Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, which it will supersede.[38] The 2008 Council Framework Decision is one of the 35 pre-Lisbon police and criminal justice measures that the UK chose to re-join in December 2014, following the exercise of the UK's block opt-out from pre-Lisbon police and criminal justice measures under Protocol 36 of the TFEU. The 2008 Framework Decision was transposed into UK law by the Criminal Justice and Data Protection (Protocol No.36) Regulations 2014.[39]

33. The 2008 Framework Decision applies to judicial cooperation in criminal matters and police cooperation. Its scope is limited to the processing of personal data transmitted or made available between Member States. The 2014 Regulations reflect this scope, applying to cross-border data processing, but not to processing activities by police and judicial authorities at a national level.

34. By contrast, the new PCJ Directive is intended to cover both cross-border and domestic processing of personal data "within the scope of EU law." The Commission justified this on the grounds that the limited scope of application of the 2008 Framework Decision was "liable to create difficulties for police and other competent authorities [who] are not always able to easily distinguish between purely domestic and cross-border processing or to foresee whether certain personal data may become the object of a cross-border exchange at a later stage."[40] As a result of the UK opt-in arrangements under Protocol 21 TFEU, and notably Article 6a of that Protocol, the Directive only applies to the UK where processing is carried out pursuant to an EU police or judicial cooperation measure in which the UK participates.[41]

35. The text of the new Directive states that it will not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, referring explicitly to activities concerning national security.[42] The

37 Q 38
38 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, (OJ L 350/60, 30 December 2008, pp 60–71)
39 The UK also re-joined Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities (OJ L 386/89, 13 December 2006, pp 89–100), which was also transposed by the 2014 Regulations.
40 Explanatory Memorandum for a Proposal for a Directive of The European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10
41 Q 56
42 Article 2(3)(a), 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 119/89, 4 May 2016, pp 89–131)

processing of personal data by Member States when carrying out activities that fall within scope of Chapter 2 of Title V of the Treaty on European Union (on the Common Foreign and Security Policy) is also outside the scope of the Directive, as is processing of data by the EU institutions and agencies.[43]

36. The European Commission says that the PCJ Directive "will ensure that the data of victims, witnesses, and suspects of crimes, are duly protected in the context of a criminal investigation or a law enforcement action." It anticipates that "more harmonised laws will also facilitate cross-border cooperation of police or prosecutors to combat crime and terrorism more effectively across Europe."[44]

37. Changes introduced by the PCJ Directive include:

- **Domestic processing:** as described above, the scope of application of the Directive will extend beyond cross-border transfers and include domestic processing of personal data (for example data transferred between two regional police forces within the UK) within the scope of EU law. This will apply to the UK only where such processing is pursuant to an EU measure on police or judicial cooperation in which the UK participates.

- **Definition of a data subject:** the Directive applies to "identified natural persons" who can be identified by physical, physiological and genetic identifiers or through online identifiers.

- **New rights of access and information for data subjects**: the Directive seeks to provide new rights of access and information for data subjects, while also permitting Member States to restrict the obligation to provide information to the data subject in specific circumstances. For example, law enforcement agencies may refuse to respond to data access requests when this is necessary in an operational context.

- **Data protection 'by design and by default'**: data controllers are obliged to implement appropriate technical and organisational measures to ensure an appropriate level of security and make sure that processing is compliant with the Directive, but are permitted to take into account practical constraints and the likelihood and severity of risk posed to the rights of data subjects.

- **Right to erasure**: the Directive includes a right for data subjects to request directly from the controller the erasure of their personal data where processing does not comply with the principles of data protection or the conditions for lawful processing.

- **Data breach notifications**: the Directive obliges data controllers to inform supervisory authorities and, in some circumstances, data subjects, of personal data breaches. Regulators must be informed no later than 72 hours after the controller has become aware of a personal data breach.

---

43 See footnote 13 above.

44 European Commission, *Agreement on Commission's EU data protection reform will boost Digital Single Market*, 15 December 2015: http://europa.eu/rapid/press-release_IP-15-6321_en.htm [accessed 11 July 2017]

- **Data Protection Officers**: the Directive obliges data controllers to appoint a Data Protection Officer, and sets out the tasks that the Officer must fulfil. However, a single Data Protection Officer may be designated for several competent authorities.

38. In evidence to our short inquiry, Professor Valsamis Mitsilegas, Professor of European Criminal Law at Queen Mary University of London, emphasised that:

> "In practice, the rights and principles in the Regulation and the Directive are the same—for example, the principle of purpose limitation or the right of access to personal data. However, the law enforcement measures contain more exceptions, to take into account the needs of law enforcement. They give national authorities greater discretion to limit the rights of individuals in certain circumstances."[45]

39. He also drew attention to the nature of the legal instrument chosen, comparing it to the GDPR, which is "one size fits all across the EU Member States." By contrast, the Directive "gives Member States breathing space: they have to implement it, taking into account their national particularities. In the field of criminal justice, this is very important."[46]

40. Rosemary Jay of Hunton and Williams highlighted "a big difference in practical application" between the Regulation and the Directive, noting that the new European Data Protection Board will have "significant authority" in enforcing the GDPR, but a lesser "advisory role" to promote consistency in relation to the Directive.[47]

41. As for the burden of implementation, Professor Mitsilegas told us he did not "see any huge burden coming forward", as "the police should have been following what is in the Directive anyway."[48]

The EU-US Privacy Shield

42. The 1995 Data Protection Directive provides that personal data can only be transferred to third countries if the third country in question can ensure an adequate level of protection. It provides for the Commission to adopt an 'adequacy decision' in order to certify that a third country can provide that standard of protection. The practical effect of an adequacy decision is that cross-border data transfers can take place without any further safeguards.

43. Under the provisions of the 1995 Directive, the Commission's adequacy decisions are subject to scrutiny by a working party composed of the representatives of national Data Protection Authorities (the Article 29 Working Party) and to approval by representatives of the Member States (the Article 31 Committee) before they can be adopted by the College of Commissioners.

44. In 2000 the Commission adopted an adequacy decision in respect of the 'Safe Harbour' framework for transferring personal data from the EU to the US. That framework had been established by the US Department of Commerce in consultation with the Commission. In 2013, the protection provided by

45 Q 10
46 Q 10
47 Q 10
48 Q 16

the Safe Harbour framework—and by extension, the Commission's adequacy decision in respect of it—was cast into doubt when Edward Snowden revealed details of the United States' PRISM surveillance programme.

45. Privacy campaigner Max Schrems asked the Irish Data Protection Commission to audit what material Facebook might be passing on to the US authorities. The case reached the Court of Justice of the European Union (CJEU). The Court interpreted the requirement for a third country to provide an adequate level of protection to mean a level of protection "essentially equivalent" to that guaranteed within the EU under the 1995 Directive.[49] The unlimited access to data by US security agencies and the limited means of redress led the Court to conclude that this standard was not met by the Safe Harbour framework. In October 2015 the CJEU declared the Commission's adequacy decision in respect of Safe Harbour invalid.

46. The Court's decision made all international transfers under the Safe Harbour framework unlawful, leading to an immediate period of legal uncertainty for companies using Safe Harbour. It also prompted further, related legal challenges by privacy campaigners, casting longer-term doubt over the legal basis for transfers of personal data from the EU to the US and, more broadly, from the EU to third countries.[50]

47. In February 2016 the European Union and the United States reached agreement on a new framework for transatlantic data transfers to replace Safe Harbour, the so-called 'Privacy Shield'. In order for data transfers to take place under the new framework, the Commission needed to adopt a new adequacy decision in respect of the Privacy Shield, which it did in July 2016. Prior to the formal adoption of the adequacy decision by the College of Commissioners, the UK had voted in favour of the draft adequacy decision at the Article 31 Committee meeting on 8 July.[51]

48. In order to join the Privacy Shield framework, US-based companies are required to self-certify to the US Department of Commerce and publicly commit to comply with the framework's requirements. While joining the Privacy Shield is voluntary, once an eligible company makes the public commitment to comply with the framework's requirements, the commitment becomes enforceable under US law.

49. The key components of the Privacy Shield framework, which superseded Safe Harbour, are:

    - **Stronger obligations on companies** certified under the Privacy Shield to protect the personal data of individuals, and more robust enforcement by the US Department of Commerce and the Federal Trade Commission. These include more explicit data retention rules, so that companies have to delete data that no longer serves the purpose for which it was collected, and an obligation to enter into written contracts

49 *Maximillian Schrems v Data Protection Commissioner* (2015) Case C-362/14

50 For example, the Irish Data Protection Commissioner has commenced proceedings to the Irish High Court seeking a referral to the Court of Justice of the European Union on the adequacy of Model Contract Clauses, which can be used as an alternative to transfers under an adequacy decision. So-called *Schrems II* case.

51 Letter from Rt Hon. Matt Hancock MP, Minister of State for Digital to Lord Boswell of Aynho, Chairman of the European Union Select Committee, 25 November 2016: http://www.parliament.uk/documents/lords-committees/eu-home-affairs-subcommittee/Matt%20Hancock%20Letter.pdf.

with any third party controller or processor where onward transfers of personal data are taking place.

- **Commitments on US government access**: written commitments have been made by the US government that access for national security and law enforcement purposes to personal data transferred to the US is subject to clear limitations, safeguards and oversight, and that bulk collection of data can only occur under specific preconditions and must be as targeted and focused as possible.

- **Redress**: new mechanisms for redress have been introduced, including the creation of an ombudsman to follow up on complaints and enquiries by EU individuals into access to data for national security purposes. The ombudsman is independent from national security services.

- **Review and Suspension**: there is provision for an annual joint review of the Privacy Shield, and a suspension clause.

50. The Privacy Shield will undergo a first annual review by the European Commission this year. Separate from this requirement, the Article 29 Working Party suggested in April 2016 that a review "must be undertaken shortly after the entry into application of the General Data Protection Regulation."[52] Under the GDPR, the general prohibition on transfers of personal data outside the EU to jurisdictions which do not provide an adequate level of protection is maintained. Adequacy decisions adopted by the Commission under the 1995 Directive remain in force "until amended, replaced or repealed." The adequacy decision on the Privacy Shield is therefore preserved, and the Regulation gives the Commission the power to make new adequacy decisions in respect of countries, sectors, territories and international organisations.

51. It is important to note that transfers of personal data outside the EU can be made in the absence of an adequacy decision, but require appropriate alternative legal safeguards, such as legally binding agreements between public bodies, model contract clauses, binding corporate rules, codes of conduct, or approved certification mechanisms.

52. This point was emphasised by Stewart Room of PricewaterhouseCoopers, who noted that only 1,700 multinationals have adopted the Privacy Shield. He told us that it was "not the default choice for US-headquartered multinationals to move data from Europe to the States. If they are using anything else, they are using the Model Contractual Clauses … Privacy Shield is still a fringe mechanism in the corporate environment."[53]

53. Rosemary Jay of Hunton & Williams qualified this by highlighting the volume of data handled by the major US suppliers of cloud storage: "Companies such as Hewlett-Packard, Google and Microsoft are all privacy-shielded. Those are big data flows."[54] The Information Commissioner also told us that, while 1,800 US companies have signed up to use the Shield, "there are many, many more in the pipeline", and that she had heard, "especially from small and medium-sized business, that this is the preferred fundamental mechanism

52 Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU-US Privacy Shield draft adequacy decision*, 13 April 2016: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf [accessed 12 July 2017]

53 Q 17

54 Q 17

for transferring data, because it is broader and more comprehensive than the standard contractual clauses."[55]

54. As for EU companies, Antony Walker, Deputy CEO of TechUK told us that the Privacy Shield was "disproportionately important for the UK within the European Union":

> "As a member of the European Union, the UK has a particularly strong relationship with the US both in terms of UK trade with the US and with the UK being a destination for foreign direct investment into the EU from the US. Compared to other EU Member States, the UK has a higher proportion of US firms that are based and located in the UK and, partly by nature of geographical position, a lot of the data transfers between the US and the EU emanate from the UK."[56]

55. Despite the scale of UK-US data transfers, the Information Commissioner told us that her office "does not record the number or types of UK data controllers who use the Privacy Shield."[57]

56. While the speed with which the Privacy Shield was negotiated, in the words of Professor Mitsilegas, "testifies to the importance of this for both sides",[58] he also noted that it "came out of the previous Administration in the US." Antony Walker warned that "we do not yet really know what the view of the new US administration is on it."[59]

57. Adding to uncertainty over the future of the Privacy Shield are the legal challenges launched against it. Mr Hancock told us he had been notified of two challenges to the Commission's adequacy decision in respect of the Privacy Shield, one led by Digital Rights Ireland, and another by La Quadrature du Net and Others. The Government had applied to intervene on the Digital Rights Ireland challenge in support of the Commission, and was "content that it is legal and that the challenges will not succeed." The Minister added that the Government would consider whether to intervene in the second case, "in support of the Commission and in defence of the agreements that have been reached. We think that the agreements that have been reached are very good."[60]

The EU-US Umbrella Agreement

58. In May 2016 the Council adopted a Decision permitting the EU to sign an international agreement with the United States on the transfer of data for criminal law enforcement purposes (the 'Umbrella Agreement'). The Agreement was signed in December 2016, after the European Parliament had given its consent, and entered into force in the EU on 1 February 2017.[61] The Agreement establishes a comprehensive framework of data protection principles and safeguards that are to apply when personal data (for example names, addresses, criminal records) is transferred between the EU (or its Member States) and the United States, "in relation to the prevention, investigation, detection or prosecution of criminal offences, including

55 Q 35
56 Q 49
57 Q 35
58 Q 17
59 Q 50
60 Q 5
61 Q 6

terrorism."[62] The Agreement's twin objectives are to ensure a high level of protection of personal data and to enhance law enforcement cooperation between the EU and the US.

59. The Umbrella Agreement does not itself authorise the transfer of personal data to the US. Rather, it sets out the overarching data protection principles and standards which should apply to existing and future data transfer agreements between the US and the EU or between the US and individual Member States for criminal law enforcement purposes. The Agreement therefore supplements existing agreements to the extent that they lack the necessary data protection safeguards. For example, it will apply to data transfers under existing agreements such as the EU-US Mutual Legal Assistance Treaty, and to existing agreements providing for the transfer of personal data by private entities for law enforcement purposes, such as the EU-US Passenger Name Records Agreement and the Terrorist Finance Tracking Programme.

60. Data transfers for national security purposes are exempt from the scope of the Umbrella Agreement. In the UK, personal data transfers to overseas partners for national security purposes are governed by the Intelligence Services Act 1994 and the Security Service Act 1989. Data transfers to third countries outside the EEA are governed by exemptions in the ministerial certificates granted to the security and intelligence agencies under section 28(2) of the Data Protection Act 1998. The Investigatory Powers Act 2016 also provides safeguards that apply when relevant material is disclosed to other countries.[63]

61. The UK's opt-in arrangements under Protocol 21 TFEU, and notably Article 6a of that Protocol, mean that the Umbrella Agreement only applies to the UK where data transfers take place under an EU agreement in which the UK participates. For example, the UK does not participate in the EU-US Mutual Legal Assistance and Extradition Agreements, and so is not bound by the terms of the Umbrella Agreement in relation to them. But it is bound by the Umbrella Agreement in respect of EU-US agreements in which it does participate, such as the EU-US Passenger Name Records Agreement. The Government's position is that the Umbrella Agreement does not cover information exchanged between the UK and the US under UK-US agreements, such as the UK-US Mutual Legal Assistance Treaty.[64]

62. Key features of the Umbrella Agreement include:

- **Limitations on data use**: personal data may only be used for the purpose of preventing, investigating, detecting or prosecuting criminal offences, and may not be processed beyond compatible purposes.

- **Onward transfers**: any onward transfer to a non-US, non-EU country or international organisation must be subject to the prior consent of the competent authority of the country that originally transferred the personal data.

---

62 Article 1, Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences (OJ L 336/3, 10 December 2016, pp 3–13)

63 Letter from the Minister of State for Digital and Culture to Lord Boswell of Aynho, 21 September 2016: http://www.parliament.uk/documents/lords-committees/eu-home-affairs-subcommittee/data-protection/dcms-lb-21-9-16.pdf

64 Q 56

- **Retention periods**: individuals' personal data may not be retained for longer than necessary or appropriate. Retention periods have to be published or otherwise made publicly available.

- **Data security breaches**: a mechanism will be put in place to ensure notification of data security breaches to the competent authority and, where appropriate, the data subject.

- **Right to access and rectification:** individuals will be entitled to access their personal data, subject to certain conditions, and will be able to request correction of data which is inaccurate.

- **Judicial Redress**: EU citizens are given the same judicial redress rights before US courts as US citizens if the US authorities deny access or rectification, or unlawfully disclose their personal data. This was achieved thanks to the Judicial Redress Act of 2016, which extended the core of the judicial redress provisions of the US Privacy Act of 1974 to EU citizens.

63. Less than a month after the Umbrella Agreement was initialled in September 2015, the CJEU ruled on the *Schrems* case. The European Data Protection Supervisor issued an opinion highlighting the CJEU's decision in *Schrems* and identifying three improvements to the text of the Umbrella Agreement that he deemed essential to ensure compliance with the Charter of Fundamental Rights and Article 16 TFEU in light of that ruling. These were, first, clarification that all the safeguards in the agreement apply to all individuals, not only to EU nationals; second, ensuring judicial redress provisions are effective within the meaning of the Charter; and third, clarification that transfers of sensitive data in bulk are not authorised. These changes were not made, as the Council took the view that the Umbrella Agreement was lawful as it stood. The Minister told us he "was and is content with this Council position."[65]

64. The Information Commissioner described the Umbrella Agreement as "a high-level set of principles that tries to create a level playing field for all the agreements and activities that come under it." It tries to "raise the standard of protection but to allow and facilitate appropriate data flows."[66]

65. Professor Mitsilegas told us that the "main advance" achieved by the Umbrella Agreement was "bringing EU law to the existing EU-US Mutual Legal Assistance Agreement." He noted that that agreement was concluded shortly after 9/11, and contained an Article (Article 9) "which says that generic differences in the data protection systems of the US and the EU should not prevent the exchange of personal data. The umbrella agreement takes it a step forward, because the United States had to provide a series of further safeguards in order for this transfer to take place."[67]

65 Letter from the Minister of State for Digital to Lord Boswell of Aynho, 19 December 2016: http://www.parliament.uk/documents/lords-committees/eu-home-affairs-subcommittee/data-protection/dcms-lb-19-12-16.pdf
66 Q 30
67 Q 18

Implications of Brexit for the UK's data protection arrangements

66. Upon leaving the EU, the UK will become a 'third country' under EU data protection rules, and will cease to be bound by EU law, including the four instruments described above.

67. The Government has said it will implement both the GDPR and the PCJ Directive in full.[68] It will need to bring forward legislation to transpose the requirements of the PCJ Directive into UK law. The Queen's Speech outlined "a new law" on data protection and "proposals for a new digital charter."[69] The Government has also said, as a general principle, that "the same rules and laws will apply on the day after exit as on the day before."[70] Notwithstanding this, the UK's data protection framework will need to be reviewed before exit in order to identify provisions that are contingent on EU membership. Those provisions would need to be amended or replaced as part of the Repeal Bill, or through dedicated legislation enacted before the date of withdrawal in order to ensure that the domestic statute book in this area is exit-proofed and can stand alone.

68. After the date of withdrawal, UK data controllers that wish to continue receiving personal data transferred from the EU[71] will have to demonstrate that they provide an adequate level of protection of personal data under Article 44 of the GDPR. In principle, this could be achieved in one of two ways:

    (a) either the UK will need to show it has data protection laws in place that are of an equivalent standard to those in the GDPR, and aim to have those recognised by the European Commission as offering adequate protection for personal data. That is, the Government would seek to obtain an adequacy decision from the European Commission under the provision in the GDPR;

    (b) or individual data controllers and processors in the UK will have to adopt their own safeguards to demonstrate that they can offer adequate protection to personal data transferred out of the EU, using the tools permitted by the GDPR, such as Standard Contract Clauses and Binding Corporate Rules.

69. Most third countries rely on the second of these options, because they have not obtained an adequacy decision from the European Commission. The Commission has thus far issued adequacy decisions under the 1995 Directive only in respect of Andorra, Argentina, the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland and Uruguay. In addition, Canada has a partial adequacy decision (in respect of commercial organisations only), and the US has an adequacy decision in respect of the Privacy Shield, such that organisations certified under the Shield need demonstrate no further safeguards in order to receive personal data from the EU.

---

68 Q 2 and Q 55

69 Cabinet Office, 'Queen's Speech 2017' (21 June 2017): https://www.gov.uk/government/speeches/queens-speech-2017 [accessed 11 July 2017]

70 Department for Exiting the European Union, *Legislating for the United Kingdom's withdrawal from the European Union*, Cm 9446, March 2017, p.5: https://www.gov.uk/government/publications/the-great-repeal-bill-white-paper/legislating-for-the-united-kingdoms-withdrawal-from-the-european-union [accessed 12 July 2017]

71 Technically the EU plus the three EEA countries that are not members of the EU: Norway, Liechtenstein and Iceland.

70. The adequacy decisions described above (based on the 1995 Directive) do not cover data exchanges in the law enforcement sector. For personal data that is subject to the Police and Criminal Justice Directive, two options would in principle be available:

    (a) either the UK will need to show it has data protection laws in place which meet equivalent standards to those in the Police and Criminal Justice Directive, and have those recognised by the Commission as offering adequate protection under Article 36 of the PCJ Directive. That is, the Government would seek to obtain an adequacy decision from the European Commission under the provision in the PCJ ;

    (b) or the exporting data controllers and processors in the police and criminal justice sector in the EU will need permission to make transfers under Article 35(1)(c) of the PCJ Directive and/or appropriate safeguards will need to be offered by the recipient UK authority. Article 37 of the PCJ Directive sets out what safeguards are permissible.

71. We asked witnesses what the default position would be, as a matter of law, for data transfers from the EU to the UK were the UK to leave the EU without having made alternative arrangements governing UK-EU data transfers. Stewart Room of PricewaterhouseCoopers said:

> "At the moment, most countries in the world do not have an adequacy decision … yet they are able to receive personal data from Europe. A range of mechanisms can be deployed or utilised to maintain the flow of data from Europe to third countries that do not have an adequacy decision … The default position is that the UK would have to rely upon these other mechanisms to maintain the movement of data from Europe into our country."[72]

72. The Information Commissioner also noted that "there are measures other than adequacy that allow data to continue flowing." For example, "companies can rely on Standard Contractual Clauses, Binding Corporate Rules, and the consent of individuals. These are all legal measures to allow and provide for the transfer of data. They are just more difficult than having an adequacy finding so that data can flow."[73]

73. Professor Mitsilegas warned that in the law enforcement field, the fall-back position was "less clear." He therefore advocated seeking a Commission adequacy decision as a means of providing certainty, "including to the law enforcement authorities of the remaining EU Member States."[74]

74. Withdrawal from the EU also has legal implications for the UK's place on relevant institutions. Ruth Boardman of Bird & Bird pointed out that once the UK is no longer a member of the EU, it will no longer be able to participate in the formal institutions that regulate data protection within the EU.[75] The Information Commissioner warned that the Information Commissioner's Office (ICO) was set to lose its place on the new European Data Protection Board and its oversight role in respect of EU institutions and agencies. Ms Denham told us: "If we leave Europol and the other arrangements and we become a third country … the impact is that the ICO—the UK's regulator—

72 Q 11
73 Q 25
74 Q 11
75 Q 51

will not have an oversight role when it comes to investigating and reviewing the very sensitive data, which could be UK citizens' data, involved in those cooperative arrangements."[76] She also noted that once the UK ceases to be an EU Member State, the ICO's relationship with the EDPB "will necessarily change", even though the decisions of the EDPB will continue to affect UK businesses providing services to European citizens.[77]

75. The Minister, Mr Hancock, refused to be drawn on the default position, as a matter of law, were the UK to leave the EU without having made alternative arrangements. He emphasised that the Government would be seeking "unhindered data flows" between the UK and the EU after Brexit, and that it was "confident of being able to achieve that."[78] He did, however, express "hope that on D+1 life will continue much as on D-1, because we have taken the decision domestically to bring the GDPR into UK law."[79] As regards data transfers for law enforcement purposes, Baroness Williams of Trafford, the Minister of State at the Home Office also refused to be drawn on the default position, noting instead that the UK's laws will be "compatible with those of the EU on the day we leave" and that the Government is "determining how best to maintain that ability to share the day after we leave the EU."[80]

76. In the next chapter, we consider the policy options available to the Government to manage the transition to a new, post-Brexit data protection regime.

76 Q 23
77 Q 26 and written evidence from the UK Information Commissioner (DPP0001)
78 Q 1 and Q 2
79 Q 4
80 Q 58

CHAPTER 3: DATA TRANSFERS AFTER BREXIT

UK-EU data transfers

The Government's aims

77. The Government has been unequivocal about the need to maintain stability and ensure "unhindered" and "uninterrupted" data flows between the UK and the EU post-Brexit.[81] Baroness Williams of Trafford, Minister of State at the Home Office, told us that "in a world of increasing mobile threats … data and data-sharing is one of our first lines of defence", and that it was therefore "absolutely vital that law enforcement agencies work together across borders to share information in order to protect the public."[82] The Government's White Paper on *The United Kingdom's exit from and new partnership with the European Union* notes that "the stability of data transfer is important for many sectors", and that the UK "will seek to maintain the stability of data transfers between the EU, Member States and the UK."[83]

78. But although the Government is clear that it wants unhindered and uninterrupted data flows with the EU post-Brexit, how it intends to achieve that goal is less apparent. Matt Hancock MP, Minister of State for Digital, told us that "there are many different ways this could work", but did "not want to stress any particular option."[84] Lady Williams has also suggested that "it is too early to say what the future arrangements might look like."[85]

79. In the meantime, the Government has announced its intention to implement the GDPR and the PCJ Directive in full, and argued that doing so will put the UK in an optimal position for the negotiations with the EU-27: "On the date of departure, the UK's data protection arrangements will be in perfect alignment with those of the continuing EU … [and] that will be a good basis for continuing negotiations", according to David Jones MP, then Minister of State at the Department for Exiting the European Union.[86] Lady Williams also emphasised the UK's "unique position" at the point of exit in being a third country "that has fully implemented the EU's provisions on data protection."[87]

Adequacy: witnesses' views

80. There was consensus among our witnesses that seeking an adequacy decision from the Commission under Article 45 of the GDPR and Article 36 of the PCJ Directive would provide the most comprehensive platform for the UK to continue receiving data from the EU post-Brexit. The Information Commissioner, Elizabeth Denham, told us that an adequacy decision would be "the best way forward" and "the most straightforward arrangement for the commercial sector and certainly for citizens and consumers."[88] Although some other countries manage without an adequacy decision, the level of

81 Q 2
82 Q 55
83 Department for Exiting the European Union, *The United Kingdom's exit from and new partnership with the European Union*, Cm 9417, February 2017, paras 8.38 and 8.40: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/589189/The_United_Kingdoms_exit_from_and_partnership_with_the_EU_Print.pdf
84 Q 2
85 HL Deb, 30 March 2017, col 732
86 HC Deb, 18 January 2017, cols 955–1023. See also Q 2.
87 Q 55
88 Q 25

integration between the UK and the EU in terms of data protection standards meant that there was "no comparator to the UK. The UK has been so heavily integrated in the EU that it is difficult to say that the UK can get by without an adequacy decision."[89]

81. Rosemary Jay of Hunton & Williams confirmed that an adequacy decision was "the strongest guarantee of the free flow of data in terms of the commercial environment."[90] Stewart Room of PricewaterhouseCoopers also saw benefit in seeking an adequacy decision, noting that it "would give certainty to businesses and to the economy."[91] He also warned that after Brexit, "the critical consideration will be the extent to which the UK is perceived to be adequate, from the EU's perspective, for data protection."[92] Mr Room listed "three key factors", which he anticipated the European Commission would take into consideration to determine whether the UK's data protection rules provided an adequate level of protection: "the overall strength of the legal framework; the effectiveness of the regulator; and [the UK's] international commitments."[93] Although both the Directive and the Regulation gave the European Commission the authority to determine that a third country did not provide an adequate level of protection, Mr Room predicted that for the UK "a declaration of non-adequacy would be surprising."[94]

82. Rosemary Jay was less sanguine. She highlighted a "popular cultural view" in Europe that the UK was "soft on regulation, including data protection", even though that perception was not borne out "on a hard analysis."[95] Ruth Boardman, of Bird & Bird, also warned that "within the EU, it will be a tough ask to persuade other … Member States … that we are the gold standard because we are widely perceived as being the pragmatic, moderating voice rather than the country which is pushing at the edge of this."[96]

83. Ms Boardman noted that when the EU had considered adequacy decisions for territories with UK-inspired data protection legislation, such as Jersey and Guernsey, "the Article 29 working party had to give an opinion on the adequacy of the laws there, and it expressed concerns about some of their

89 Q 25
90 Q 11
91 Q 11
92 Q 10
93 Article 45, Regulation (EU) 2016/679 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 119/1, 4 May 2016, pp 1–88) and Article 36, Directive (EU) 2016/680 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 119/89, 4 May 2016, pp 89–131) list three areas which "the Commission shall, in particular, take account of" when assessing the adequacy of the level of protection. These are "(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral …as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation …case law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects … (b) the existence and effective functioning of one or more independent supervisory authorities in the third country …with responsibility for ensuring and enforcing compliance with the data protection rules…(c) the international commitments the third country …has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data."
94 Written evidence from Stewart Room (DPP0002), para 17 and 24
95 Q 13
96 Q 47

laws precisely because they replicated UK law." She emphasised that while the UK was a member of the EU, it was "automatically adequate", but such instances showed that the UK was "not seen as being the gold standard."[97]

84. There is a paradox here, in that higher standards of data protection may be required of third countries than are required of EU Member States. When considering an adequacy decision, the European Commission will look at a third country's data protection framework in the round, including looking at national security legislation (which is a national competence for EU Member States). As Ruth Boardman noted, as long as the UK is a member of the EU, "national security concerns cannot be used as a reason to prevent a free flow of data" with the EU. However, once the UK in no longer a member of the EU, national security concerns "could be used as a reason for arguing that the UK ought not to be adequate."[98]

85. Professor Mitsilegas pointed out that, since the ruling in the *Schrems* case, the CJEU had been "raising the bar on adequacy":

> "The Court of Justice in *Schrems*—which involved the US so we are not talking about some third country with no system—said that the two systems need to be essentially equivalent. The Court said … that it is not enough to tick-box the legislation. You have to examine how this works in practice and ensure that data protection is provided in an effective manner. The benchmark is high."[99]

86. Professor Mitsilegas also highlighted the ongoing role of the CJEU and the continued relevance of the Charter of Fundamental Rights in relation to adequacy decisions:

> "In the field of data protection, we should not forget that the Court of Justice interprets the instruments, the Regulation and the Directive, in conformity with the EU Charter of Fundamental Rights, which is part of the EU law … This means that compatibility, equivalency or adequacy under the Data Protection Directive or Regulation will be assessed by the Commission in light of the interpretation of these instruments by the Court of Justice. However you define the legal relationship and the impact of the court … the Court of Justice's case law must be taken into account."[100]

87. The Government is non-committal about whether it plans to seek an adequacy decision. Mr Hancock acknowledged that "an adequacy decision could work" as a way of achieving the Government's objectives, but emphasised that there were "many different ways in which you could make this work."[101] Lady Williams told us that "an adequacy agreement is certainly an option, but I cannot say, in the context of other options that might be available, what the end point will look like."[102]

97 Q 47
98 Q 51
99 Q 11
100 Q 12
101 Q 2
102 Q 60

Alternatives to adequacy: witnesses' views

88. There was consensus among our witnesses that although alternatives to an adequacy decision are available, those alternatives would be less effective in reducing friction around data flows. The Information Commissioner, Elizabeth Denham, told us that alternative mechanisms were "not as broad, all-encompassing and clear as an adequacy agreement", and "not as straightforward."[103] Antony Walker, of TechUK, told us that the impact of not having an adequacy decision would be felt "economy-wide", and listed a series of drawbacks:

> "The first would be a significant increase in the amount of red tape that businesses have to deal with as they would have to put other mechanisms in place to lawfully transfer data. That means cost because there will be significant legal costs associated with putting those measures in place. There is also an element of uncertainty which is about the future legality[104] of some of the mechanisms … Finally, there is an issue around competitive disadvantage for UK firms. If [UK] firms have to jump through a whole set of additional legal hoops in order to transact and do business with firms or customers across the European Union, they will be at a disadvantage versus their competitors who are based in the European Union and do not have to go through all those steps."[105]

89. Under the GDPR, in the absence of an adequacy decision data transfers can take place to a third country or international organisation only if the data controller or processor has appropriate safeguards in place, and "enforceable data subject rights and effective legal remedies for data subjects are available."[106] Box 2 sets out the alternative legal mechanisms permissible under the GDPR.

103 Q 25
104 See paras 46, 93 and 115 on the *Schrems II* case.
105 Q 44
106 Article 46(1), Regulation (EU) 2016/679 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/E (OJ L 119/1, 4 May 2016, pp 1–88)

Box 2: Data Protection Safeguards under Article 46 of the GDPR

Under Article 46 of the GDPR, the following mechanisms constitute appropriate safeguards, without requiring any specific authorisation from a supervisory authority:

- A legally binding and enforceable instrument between public authorities and bodies;
- Binding Corporate Rules;
- Standard Contract Clauses adopted by the Commission;
- Standard Contract Clauses adopted by a supervisory authority and approved by the Commission;
- An approved Code of Conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards;
- An approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards.

Mechanisms are also available under the GDPR for transferring data, subject to authorisation from the competent supervisory authority. These are:

- Contractual clauses between the controller or processor and the controller, processor or the recipient of the data;
- Provisions that are inserted into administrative arrangements between public authorities or bodies, and which include enforceable and effective data subject rights.

Source: Article 46 (2) (a)-(f) and 46 (3) (a) and (b) of Regulation (EU) 2016/679 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 119/1, 4 May 2016)

Standard Contract Clauses and Binding Corporate Rules

90. The main mechanisms in the GDPR permitting data transfers out of the EU to countries or organisations that are not covered by an adequacy decision are Standard Contractual Clauses (SCCs)[107] and Binding Corporate Rules (BCRs).[108] Our witnesses agreed that although these mechanisms were less good than an adequacy decision, they did provide a viable alternative in some cases. Ruth Boardman told us that SCCs were "the most commonly used way of transferring data because [they require] less effort … you sign a contract and then you have a mechanism for transferring data."[109]

91. The Information Commissioner raised concerns that mechanisms like SCCs would "not [be] easy for businesses, particularly small and medium-sized businesses."[110] Antony Walker agreed that SMEs, would face "significant

107 SCCs are also sometimes referred to as Model Contracts or Model Clauses.
108 Article 46, Regulation (EU) 2016/679 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 119/1, 4 May 2016, pp 1–88) lists other options as mentioned above (see Box 2) but our witnesses identified these two as the main mechanisms for third countries and organisations to transfer data in the absence of an adequacy decision.
109 Q 44
110 Q 25

legal costs associated with putting [SCCs] in place."[111] Such mechanisms would be "a significant impediment to doing cross-border trade" and a "significant disincentive" for SMEs to expand into international markets or partner with other firms in other markets.[112] Ms Boardman told us that even for larger organisations, SCCs added "cost and complexity."[113]

92. Ruth Boardman also noted that SCCs were not a practical option for businesses that sell directly to consumers in the EU. In such cases, "there will not be two parties to enter into the contract", meaning that SCCs were "not really possible for that kind of organisation."[114]

93. Antony Walker and Ruth Boardman were also concerned that SCCs could potentially be precluded by virtue of an ongoing legal challenge initiated by Max Schrems.[115] Ms Boardman told us this could be "particularly significant for the UK because, if those data transfer agreements are held to be invalid, the main alternative way that businesses would use to allow data to be shared with the UK would suddenly cease to be valid."[116] Antony Walker added that you could "quite quickly" get into "a scenario where you run out of options",[117] while Ruth Boardman noted that data flows could be "massively disrupted."[118]

94. BCRs are designed to allow a multinational company, or a group of companies, to transfer data from the EU to their affiliates outside the EU. Ruth Boardman told us that BCRs required "fairly sophisticated approaches to data protection", making them difficult for SMEs.[119] Moreover, the participating company's data protection standards would have to be authorised by a data protection authority, which required a "presence in an EU member state." This meant that "if you are just a UK company, you could not use that mechanism."[120] Antony Walker highlighted the case of one company that had been seeking authorisation for its BCRs "for more than five years" and had still not received authorisation, casting doubt on whether BCRs could offer a prompt solution for UK firms in the absence of an adequacy decision.[121]

111 Q 45
112 Q 45
113 Q 45
114 Q 45
115 On 31 May 2016 the Irish Data Protection Commissioner (DPC) commenced proceedings in the Irish High Court to seek a reference to the CJEU as to the validity of the SCC mechanism. This case has its roots in a complaint about Facebook made to the DPC by privacy advocate Max Schrems in 2013 in light of disclosures made by Edward Snowden about the US Government's PRISM programme. As of 16 March 2017 the Irish High Court had not delivered its ruling as to whether or not a reference should be sought from the CJEU. See Data Protection Commissioner, *Update on litigation involving Facebook and Maximillian Schrems: Explanatory Memo*, (16 March 2017): https://www.dataprotection.ie/docs/16-03-2017-Update-on-Litigation-involving-Facebook-and-Maximilian-Schrems/1598.htm [accessed 10 April 2017]
116 Q 44
117 Q 46
118 Q 46
119 Q 46
120 Q 46
121 Q 46

Box 3: Data Protection Safeguards in the PCJ Directive

Under the PCJ Directive, data transfers can take place in the absence of an adequacy decision to a third country or international organisation where "(a) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or (b) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data."[122] In the absence of both an adequacy decision and appropriate safeguards, the Directive allows for derogations for specific situations under which Member States may still transfer data for law enforcement purposes. These are:

- To protect the vital interests of the data subject or another person;
- To safeguard legitimate interests of the data subject, where the law of the Member State transferring the personal data so provides;
- For the prevention of an immediate and serious threat to public security in a Member State or a third country;
- In individual cases for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security; or
- In an individual case for the establishment, exercise or defence of legal claims relating to the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security.[123]

Source: Article 37 (1) (a)-(b) and 38 (1) (a)-(e), Police and Criminal Justice Directive (OJ L 119/89, 4 May 2016, pp 89–131)

95. Professor Mitsilegas warned that, while there might be viable alternatives to an adequacy decision in the commercial sphere:

> "In the field of law enforcement, things become more complicated, because even if the United Kingdom wanted to proceed into bilateral agreements with EU member states, when EU member states act externally they are bound by EU law. They cannot cooperate with third countries if these countries are not perceived to provide an equivalent level of protection. There, I think, adequacy would be more important for the UK and for public security."[124]

96. As for other alternatives, trade agreements have recently emerged as a means of regulating cross-border data flows. One example is the Trans-Pacific Partnership Agreement (TPP), which imposes limits on the extent of data

122 Article 37(1)(a)-(b), 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 119/89, 4 May 2016, pp 89–131)

123 Article 38(1)(a)-(e), 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 119/89, 4 May 2016, pp 89–131)

124 Q 11

protection regulation that signatories can provide in their national laws.[125] Antony Walker suggested that if the UK was not "really committed" to seeking an adequacy decision, it could seek "a new treaty arrangement" with the EU, either as part of the "overall new relationship or in a specific data protection treaty."[126]

Timings and transition

97. The Government appears to envisage uninterrupted data flows, with data transfers the day after withdrawal continuing much as before.[127] The Information Commissioner agreed that "if there is a way to negotiate either a transition arrangement or something so that there is not a cliff-edge on day one, that is in the best interests of everyone."[128] However, she also questioned whether this would be feasible: "Achieving adequacy on day one after exiting the EU may be challenging because there is a legal process involved."[129] Rosemary Jay emphasised that reaching an adequacy decision was "a legislative process", and that it was "not simply within the [Commission's] gift to [deliver an adequacy decision] in some informal way."[130] She could "see no way" to foreshorten the process, noting that under EU law the UK needed to become a third country before it could be subject to an adequacy decision.[131]

98. Other witnesses raised concern about the length of time it might take to secure an adequacy decision. Stewart Room noted: "The point about there being only nine [jurisdictions that have adequacy decisions from the EU] is also an indicator of the amount of time and complexity that attaches to the development of an adequacy decision."[132] Adequacy decisions could "take many years" to negotiate.[133] Antony Walker agreed that it was "quite a lengthy process", which would "take in the range of about two years to go through the various stages."[134] Mr Walker also warned of a "real risk" that legal challenges before the CJEU could coincide with the end of the Brexit negotiations, leading to "real uncertainty."[135]

99. Stewart Room acknowledged the challenge of sequencing, but emphasised that "the mutual interest is absolutely clear."[136] He suggested that "the essential point about data protection is that all of Europe … believes in [it] … There is an interest for all EU member states to maintain strong data protection. The 27 would want to see strong data protection for their citizens who remain in [the UK] afterwards."[137]

100. Antony Walker also identified a shared interest in managing the transition: "There are many businesses across the European Union which are just as

125 UNCTAD, *Data protection regulations and international data flows: implications for trade and development*, (2016), p37: http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1468 [accessed 5 July 2017]
126 Q 53
127 Q 4
128 Q 25
129 Q 25
130 Q 12
131 Q 12
132 Q 11
133 Q 11
134 Q 45
135 Q 46
136 Q 13
137 Q 12

concerned that there is a smooth transition as UK firms are." He therefore hoped that transition could "be managed in a positive way" and emphasised the need for a transitional agreement to avoid a 'cliff-edge'. [138] He wanted "to see an extension of current processes up until the point that a new relationship enters into force."[139]

UK-US data transfers

Onward transfers: interaction between EU and US arrangements

101. The type of agreement that the UK establishes with the EU to facilitate UK-EU data transfers after Brexit may also affect data flows between the UK and other third countries. An adequacy decision would require the UK to transfer the personal data of EU data subjects only to countries or organisations that meet EU data protection standards. The Information Commissioner, Elizabeth Denham, explained: "If the Government decide to proceed and obtain an adequacy finding for the UK as a third country, that will limit how much manoeuvre we have", adding that "when you bind yourself to an adequacy decision, the European Commission will put constraints in place."[140] Stewart Room agreed that in order to receive an adequacy decision from the EU, the UK might "have to put up some barriers in relation to third countries."[141] As Ruth Boardman put it:

> "If the UK gets adequacy, it is a ship in which it is safe to put EU data. If our rules on onward transfers are too lax, then there are lots of holes in the ship and that data can escape, so it affects your own adequacy decision. That is an incentive … for trying to follow the EU approach very closely, unless there is a good reason to depart from it."[142]

102. These factors will be relevant when the Government considers whether to replace the EU-US Privacy Shield and the EU-US Umbrella Agreement, which will cease to apply to the UK when it ceases to be a member of the EU.

The Government's aims

103. The Government's objective for UK-US data transfers is similar to its objective for UK-EU data transfers. The Minister told us:

> "We must have a view both on our future position with the EU and on our future position with other jurisdictions that have high-quality data protection regimes, the US being the most obvious example. We must make sure that we have a free flow of data with them, too. Currently, we do that through the EU, but we will have to do it directly instead."[143]

Replacing the EU-US Privacy Shield: witnesses' views

104. Currently UK and US organisations share data either via mechanisms such as SCCs and BCRs or under the EU-US Privacy Shield. The Privacy Shield will no longer apply to the UK post-Brexit, and we therefore asked whether the UK would need to replace it with an equivalent agreement between the UK and the US.

---

138 Q 45
139 Q 45
140 Q 29
141 Q 11
142 Q 48
143 Q 2

105. The Information Commissioner, Elizabeth Denham, was clear that "[we] will need to strike our own agreement with the US."[144] Ruth Boardman observed that many of the firms that had signed up to the EU-US Privacy Shield from the US were "large firms that are doing large volumes of data transfer"; she saw the Privacy Shield as "the easiest mechanism to enable UK- and US-based firms to transfer data lawfully."[145] The Information Commissioner stressed that for SMEs in particular the Privacy Shield was better than the alternatives, such as SCCs.[146]

106. Rosemary Jay suggested Switzerland as a possible model for the UK: "Switzerland has an adequacy finding, so it is regarded as equivalent and adequate, and then it has a mirror of the Privacy Shield agreement with the US."[147] This meant that the "flow of data from Europe through to Switzerland, through to the US and back round again is unimpeded"[148] The Information Commissioner also saw merit in the Swiss model, and did not see why the UK would need to "completely reinvent the wheel."[149] Professor Mitsilegas noted that if the UK had an adequacy decision from the EU, the Government could even propose a "tripartite venture" with the EU and the US.[150]

Replacing the EU-US Umbrella Agreement: witnesses' views

107. Asked whether the UK should seek an umbrella-style agreement with the US, the Information Commissioner told us: "Any arrangement that gives us a strong harmonised approach for protection of personal data and facilitates the appropriate transfer of data is a good thing."[151] Baroness Williams of Trafford, Minister of State at the Home Office, told us that the Government intended to "explore what we do going forward."[152]

US approach: witnesses' views

108. We also asked whether there would be appetite from the US to conclude either a privacy shield-type agreement or an umbrella-type agreement with the UK. The Information Commissioner described the question as "theoretical" at this stage.[153] For law enforcement, she emphasised that having something in place would be "fundamentally important", and that she "would expect the public to want us to all get on with this and make sure [that] data is protected."[154] Antony Walker, of TechUK, noted that "data protection and privacy and so on are becoming fundamental enablers to trade", and suggested that there might be some appetite to include data protection in a UK-US free trade agreement.[155] However, Mr Walker warned that "We simply do not know what US trade policy is going to be yet", and that it was "too early to judge."[156]

---

144 Q 35
145 Q 49
146 Q 35
147 Q 17
148 Q 17
149 Q 35
150 Q 17
151 Q 36
152 Q 65
153 Q 35
154 Q 36
155 Q 50
156 Q 50

109. Professor Mitsilegas told us that the attractiveness of a UK-US Privacy Shield for the US would partly depend on the "commercial interests" at stake.[157] Antony Walker noted that "compared to other EU member states, the UK has a higher proportion of US firms that are based and located in the UK and … a lot of the data transfers between the US and the EU emanate from the UK."[158]

Conclusions and recommendations

110. **The Government has said that it wishes to secure unhindered and uninterrupted flows of data between the UK and the EU post-Brexit, to facilitate both trade and law enforcement cooperation. We support this objective, and note that any arrangement that resulted in greater friction around data transfers between the UK and the EU post-Brexit could hinder police and security cooperation. It could also present a non-tariff barrier to trade, particularly in services, putting companies operating out of the UK at a competitive disadvantage. The Government must not only signal its commitment to unhindered and uninterrupted flows of data, but set out clearly, and as soon as possible, how it plans to deliver that outcome. We were struck by the lack of detail in the Government's assurances thus far.**

111. **There was consensus among our witnesses that the most effective way to achieve unhindered flows of data would be to secure adequacy decisions from the European Commission under Article 45 of the General Data Protection Regulation and Article 36 of the Police and Criminal Justice Directive, thereby confirming that the UK's data protection rules offered an equivalent standard of protection to that available within the EU.**

112. **Although other legal mechanisms to facilitate cross-border flows of data are available, we were persuaded by the Information Commissioner's view that the UK is so heavily integrated with the EU—three-quarters of the UK's cross-border data flows are with EU countries—that it would be difficult for the UK to get by without an adequacy arrangement. We therefore recommend that the Government should seek adequacy decisions to facilitate UK-EU data transfers after the UK has ceased to be a member of the EU. This would provide the least burdensome and most comprehensive platform for sharing data with the EU, and offer stability and certainty for businesses, particularly SMEs.**

113. **Adequacy decisions can only be taken in respect of third countries, and there are therefore legal impediments to having such decisions in place at the moment of exit. In the absence of a transitional arrangement, this could put at risk the Government's objective of securing uninterrupted flows of data, creating a cliff-edge. We urge the Government to ensure that any transitional arrangements agreed during the withdrawal negotiations provide for continuity of data-sharing, pending the adoption of adequacy decisions in respect of the UK.**

157 Q 17
158 Q 49

114. **In the absence of such transitional arrangements, the lack of tried and tested fall-back options for data-sharing in the area of law enforcement would raise concerns about the UK's ability to maintain deep police and security cooperation with the EU and its Member States in the immediate aftermath of Brexit.**

115. **The need for transitional arrangements also extends to the commercial sector. Although there are alternative mechanisms to allow data to flow out of the EU for commercial purposes, these are sub-optimal compared to an adequacy decision, and may not be available to some types of companies, for instance small companies or those dealing directly with consumers. Some are also currently subject to legal challenge, notably the *Schrems II* case against Standard Contractual Clauses, underlining the need for a transitional arrangement.**

116. **The EU-US Privacy Shield and the EU-US Umbrella Agreement will cease to apply to the UK post-Brexit. Because of EU rules for onward transfers, securing unhindered flows of data with the EU may require the UK also to demonstrate that it has put arrangements in place with the US that afford the same level of protection as the Privacy Shield and the Umbrella Agreement. As regards data-sharing for commercial purposes, we note the approach taken by Switzerland, which has secured both an adequacy decision from the EU and a mirror of the Privacy Shield agreement with the US.**

CHAPTER 4: UK DATA PROTECTION POLICY AFTER BREXIT

Room for manoeuvre on UK data protection policy after Brexit

117. Even if the UK's data protection regime is aligned with the EU regime to the maximum extent possible when the UK leaves the EU, there is the prospect that over time the EU will amend or update its rules, not least as the GDPR and the PCJ Directive both mandate reviews by the Commission every four years. The UK will be free to choose whether to align itself with any changes in EU law, but failure to do so could have consequences for the UK's 'adequacy' status (assuming such a status has been secured). The same considerations may apply in choosing whether to follow the EU's lead in recognising third countries or international organisations as providing adequate protection for the transfer of personal data, or in repealing or suspending such recognition.

'White Space' in the GDPR

118. The Information Commissioner told us:

> "If the Government decide to proceed and obtain an adequacy finding for the UK as a third country, that will limit how much manoeuvre we have. We will have to keep our laws up to an equivalent standard, which will be assessed every three or four years. There will be some constraints around that."[159]

119. She emphasised, however, that in the meantime the GDPR itself had "a lot of white space" in it: "There is still a lot of room for manoeuvre so that domestic authorities can carve out and make the laws they want." The Information Commissioner cited the UK's ability to make decisions at a domestic level "on children and age of consent and on balancing freedom of expression and the role of the media with data protection."[160]

120. Stewart Room of PricewaterhouseCoopers also drew attention to "white space" within the GDPR, which would allow the UK to develop policy within the overall framework of the Regulation. Mr Room told us that "most of the things that businesses and other organisations will have to do operationally … are not yet described in the GDPR … they will have to come from somewhere. The primary source will be via regulatory guidance, for instance." He concluded that there was "very significant space inside the GDPR framework for the United Kingdom to develop its positions for day-to-day operationalisation of this subject matter", and suggested that "if the UK fills that white space via a strong regulator and industry bodies, we can have a data protection framework that in practical terms has been designed by the UK."[161]

121. Rosemary Jay of Hunton & Williams highlighted what she saw as "scope within the GDPR framework for us to continue focusing on those things—for example, medical research—where we have huge resources and capacity, and to continue leading the way in areas such as fraud assessment and prevention."[162] She noted that there were "quite wide exemptions for

159 Q 29
160 Q 29
161 Q 14 and Q 19
162 Q 14

research", which would offer leeway to maintain support for medical research in oncology, for example, where the UK was already world-leading.[163]

122. Some of the 'white space' in the GDPR will be filled in by EU institutions, rather than Member States. The Information Commissioner noted that the Regulation contains many trigger terms such as 'high-risk', 'large scale', and 'systematic,' and that until the new European Data Protection Board and the courts start interpreting these terms "it is not clear what the GDPR will look like in practice."[164]

Regulatory Divergence

123. The Minister, Matt Hancock MP, noted that "if the rest of the European Union, once we had left, chose to change its data rules, we would have to decide whether to change ours to mirror them—because there are advantages to being the same as the European system—or whether to maintain a slightly different system." He anticipated that the UK would have to "make that decision at the time, according to what the changes are", and that while "there is the potential to make the GDPR easier to comply with or more flexible … we would want to do that only consistent with maintaining unhindered data flows."[165]

124. The Minister drew a parallel with the UK's relationship with other major economies: "If the US changes its data rules now, the EU—and, in future, we and the EU—has to think about whether to update its own rules." He predicted that the UK would need "a set of global relationships, rather than relationships only at a European level", and emphasised that "the UK domestic government will be able to decide the changes that we make domestically, given everybody else's position."[166]

125. Antony Walker of TechUK argued that "the best thing for the UK economy and for UK citizens is to stay closely harmonised with European law." He conceded that "over time, areas might emerge where it makes sense to diverge", but argued that "we would have to make a very careful analysis of the pros and cons of diverging and, if the impact of diverging meant that an adequacy agreement would not be possible or would no longer be valid, you would have to question very carefully whether that was the right thing to do."[167]

126. Ruth Boardman of Bird & Bird accepted that the GDPR was "not perfect", and highlighted "opportunities to alter things and do things better in the medium term", but warned that trying to do so in the short term could be "hugely unsettling; it stops you planning, you have too much change and it risks impacting on adequacy."[168]

127. Mr Room told us that it was "plainly in the interests of our economy, if we want to trade with Europe, to be on the same platform. If we do not, we run the risk of a judicial decision by the Court of Justice [of the European Union] that prevents the flow of data into our country from Europe. That will have

163 Q 14
164 Written evidence from Elizabeth Denham (DPP0001)
165 Q 4
166 Q 4
167 Q 48
168 Q 53

a serious impact."[169] Rosemary Jay of Hunton & Williams also focused on the UK's trading relationships:

> "If we wanted to carve out a different place in the world, have different trading partners and not focus on trade with Europe and the US, we could do what we wanted. It is not absolutely inevitable. We can pass whatever data protection law we want, but in consequence it would be extremely difficult to have a finding of adequacy or to build the equivalent of a Privacy Shield."[170]

128. Antony Walker of TechUK emphasised that global companies would want to put in place "a single set of processes":

> "If you are running global operation, you will want to have consistent processes across your businesses. What we are seeing is that global firms based outside of the EU are taking the GDPR as the norm for their business and are building their processes around it, so, for very large companies, there is no desire to diverge from the GDPR—the opposite, because they worry about falling between the gaps."

An important factor in this respect, Mr Walker suggested, was the introduction of "very significant new fines" in the GDPR.[171] He concluded that overall, "businesses would like to see a settled regulatory framework", and that "stability is good …This is the constant message that we get back from our members, large and small."[172]

129. As for future evolution, Mr Walker predicted there would be constraints on the UK's ability to innovate with regulation in this area: "We can try to be at the forefront of thinking about how things need to change, but we would need to bring the rest of the European Union with us, and it is not clear to me exactly how we would do that." He stressed that "we have to remember the size of the UK market versus the size of the European market", which meant that "we will have to do that very much in partnership with the European Union, rather than simply boldly striking out by ourselves and hoping others will follow."[173]

130. Mr Room emphasised the importance of the UK having a "practical influence, with an embassy or whatever it might be" in Brussels, and "a strong regulator, so we do not allow ourselves to diverge in such a way that people can attack the UK's adequacy."[174] Mr Walker also made the case for a dynamic process of review: "We do not want to see a process of accidental divergence happening as the European Union continues to legislate in areas where the UK does not. There needs to be a process that enables us to carefully track what is happening at a European level and to determine whether or not those changes should be implemented into UK law."[175]

---

169 Q 19
170 Q 19. Note in this context that the UK has ratified the Council of Europe Data Protection Convention of 1981 (known as Convention 108) and so any data protection laws passed by the UK would still have to comply with the Convention, which is binding on its signatories.
171 Q 47
172 QQ 47 and 53
173 Q 47
174 Q 21
175 Q 48

131. Ruth Boardman drew particular attention to the EU's adequacy decisions in respect of third countries and organisations, noting that because the UK will have implemented the GDPR, "we will need a mechanism to judge countries as being adequate", and arguing that "it would be sensible to allow the UK to follow EU decisions."[176]

Reviews of 'adequacy'

132. Professor Mitsilegas noted the requirement in the GDPR and the PCJ Directive for the Commission to review its adequacy decisions as part of the four-yearly review process. He noted that in the case of *Schrems*, "the problem was that the Commission [had] made an adequacy decision many, many years ago, and the Court said, 'How do you know what is going on now? You need to check at regular intervals." The Commission would in future be "obliged … to check regularly", and this meant that countries that wanted an adequacy decision needed to prepare for sustained scrutiny of their own data protection framework.[177]

Privacy vs security

133. Continuing UK alignment with EU data protection laws could come into tension with the Government's preferred approach to data retention and surveillance for national security purposes. While the UK remains a member of the EU, national security is the sole responsibility of each Member State, as outlined in the TFEU (Article 4.2). However, the boundaries between Member State competence over national security and EU competence over data protection and retention are increasingly being tested before the CJEU.[178]

134. For example, in the recent *Tele 2 and Watson* case,[179] challenges were brought in Sweden and the UK against domestic legislation that imposed an obligation on communications providers to retain traffic and location data, questioning whether the obligations in question were compatible with EU data protection law. In the UK, the legislation being challenged was the Data Retention and Investigatory Powers Act 2014 (DRIPA), which has since expired and been replaced by the Investigatory Powers Act 2016. The CJEU gave its interpretation of what EU law requires in December 2016.[180] It is now for the domestic courts to rule on the lawfulness of the domestic legislation in question. Lady Williams told us that:

> "The judicial review proceedings concerning the Data Retention and Investigatory Powers Act 2014—aka DRIPA—have not yet concluded. We are currently waiting on the Court of Appeal's response to the CJEU December 2016 judgment. However, in the light of the CJEU judgment, and in order to bring an end to the litigation, the Government have accepted to the Court of Appeal that the Act was inconsistent with EU law in two areas."[181]

176 Q 48
177 Q 11
178 See for example *Stefano Melloni v Ministerio Fiscal* (2013) C-399/11 and *N.S v Secretary of State for the Home Department and M.E and Others v Refugee Applications Commissioner* (2011) C-411/10
179 *Tele2 Sverige AB v Postoch telestyrelsen* (2016) Case C-203/15 and Case C-698/15, *R v Secretary of State for the Home Department ex p David Davis MP, Tom Watson MP, Peter Brice and Geoffrey Lewis* (2015) EWCA Civ 1185. David Davis MP has had to recuse himself from the legal challenge having been appointed to the UK Government in July 2016.
180 Preliminary Ruling, 21 December 2016: *Tele2 Sverige AB v Postoch telestyrelsen* (2016) Case C-203/15 and Case C-698/15
181 Q 66

135. Although DRIPA 2014 has expired, the CJEU's ruling potentially has ramifications for the Investigatory Powers Act 2016, which contains similar provisions. Mr Hancock told us that, notwithstanding the CJEU's verdict on DRIPA, the Government was "confident that the Investigatory Powers Act [which replaced DRIPA] is consistent with the GDPR."[182]

Relevance of UK domestic legislation

136. As we noted in Chapter 2, if the UK were to seek an adequacy decision from the Commission post-Brexit, its data protection standards would be assessed without the benefit of the protection afforded by the national security exemption in the TFEU. Not only would the UK's law and practice on data retention and surveillance for national security purposes become relevant to any initial assessment of adequacy by the Commission, but any future change in national practice could potentially affect the UK's adequacy status.

137. Professor Mitsilegas suggested that the UK was "going down this route of increasing collection of and access to bulk data, which is increasingly incompatible with the EU."[183] He predicted that "in the field of security there may be challenges for the UK if EU Member States and the Commission perceive that UK data protection law is of a lower standard than EU law as interpreted by the Court of Justice."[184]

138. The Information Commissioner emphasised that the courts were now doing some of the balancing between privacy and public safety or law enforcement, and that the involvement of the courts was "something that governments cannot control."[185] She anticipated that the Court of Appeal's decision in the *Tele2 and Watson* case would be "telling" and "important for us to take into account for our domestic law." Based on recent CJEU judgments, the Commissioner judged that "it seems likely that the UK's surveillance and data retention regime would be a risk for a positive adequacy finding." She consequently identified this as "an area of tension … I am hoping it is resolvable."[186]

EU perception of UK practice

139. Rosemary Jay of Hunton and Williams noted that in transcripts from the *Schrems* court hearing, "there is occasionally a flavour to the comments that seems to suggest that Ireland and the UK do not take this as seriously somehow."[187] Professor Mitsilegas suggested there was a "differentiated picture", with standards on the regulation of private companies perceived as "quite close together", while in the field of security, "there are concerns about the United Kingdom."[188] He judged that "mass surveillance on the basis of bulk collection of personal data and the transfer of this data to the law enforcement authorities … is a red line for EU law now", and predicted that "as long as you have domestic law that allows mass surveillance, you will have problems with EU law." He emphasised that this was "not exactly the same as saying that the UK does not have adequate data protection supervision mechanisms in its own system. It does, but when you have

182 Q 7
183 Q 21
184 Q 12
185 Q 30
186 Q 37
187 Q 13
188 Q 13

political choices that say that more and more personal data should be collected indiscriminately, this causes problems for EU law."[189]

Partial adequacy findings

140. Given the potential tension between the UK's data retention and surveillance regime and EU data protection law as interpreted by the CJEU, we asked whether this could lead to a partial adequacy finding, with the UK being ruled adequate on commercial data but not on data protection in law enforcement, for example. Rosemary Jay told us that the GDPR had now formalised the concept of a partial adequacy finding, and that "it is possible that there is more flexibility than there has been previously."[190]

141. Ruth Boardman, though, predicted that in the case of the UK, an adequacy finding would be "kind of all or nothing, and the reason why it might be nothing would be if there was no political will or if our national security legislation precluded an adequacy decision."[191] The Information Commissioner judged that while "partial adequacy is better than no adequacy", the best way forward was to have a "unified, harmonised approach across all sectors", and she therefore advocated a "more assertive" approach, seeking full adequacy.[192]

UK influence on data protection standards in the EU and beyond

142. We also explored whether and how the UK's influence on data protection standards in the EU and elsewhere might change as a result of Brexit. Our witnesses emphasised that the UK had already exerted considerable influence on EU regulation, and the Minister, Mr Hancock, told us that "the UK voice remains influential" at the EU level in a range of areas, including data protection.[193] The Information Commissioner told us that the UK has been "front and centre" in the development of the GDPR and the PCJ Directive, and that the UK had "a lot to be proud of in our contributions to the protection of personal data."[194]

143. Mr Hancock highlighted specific occasions when the UK had been influential, citing recent discussions on data localisation, where the UK "managed to get an overwhelming majority of countries" to oppose the principle of data localisation (rules stipulating that data must be stored locally).[195] On data-sharing for law enforcement purposes, he told us that "effective data-sharing with our international partners, both EU and non-EU, will remain a top UK priority", and set out his expectation that the UK would "play a leading role in that, as we do now."[196] However, Ministers were less clear about precisely how they planned to sustain the UK's influence after Brexit, beyond stating

189 Q 13. As regards supervision mechanisms within the UK's own system, see for example Section 227 of the Investigatory Powers Act 2016 provides for the appointment of an Investigatory Powers Commissioner, whose role is to authorise and oversee the use of Investigatory Powers by public authorities. See Prime Minister's Office, 'Investigatory Powers Commissioner appointed: Lord Justice Fulford' (3 March 2017) https://www.gov.uk/government/news/investigatory-powers-commissioner-appointed-lord-justice-fulford [accessed 11 July 2017]
190 Q 21
191 Q 51
192 Q 41
193 Q 2
194 Q 27
195 Q 2
196 Q 6

that "it is in our interests and in those of the EU that … cooperation … continues."[197]

144. Antony Walker, Deputy CEO of TechUK, also judged that the UK had promoted its interests effectively. He told us that the UK had been "extremely influential" at the EU level in "establishing the principles and the framework that underpin data protection legislation."[198] His counterparts in Europe and within EU institutions viewed the UK's input on [data protection] as being "extremely important … I would argue that the UK has been influential in shaping legislation."[199]

145. The UK has also been actively engaged in discussions about data-sharing and surveillance for law enforcement purposes. Professor Mitsilegas told us that the UK was "instrumental" in encouraging other Member States to "increase access to personal data by law enforcement authorities", and had been "very influential" in getting other Member States to expand surveillance.[200] He noted that the UK had "advocated strongly" for the Directive on Passenger Name Records,[201] and that the Data Retention Directive[202] "was a UK initiative."[203] He predicted that "the UK absence from the negotiating table will be a loss for the EU and the other Member States."[204]

146. The loss of the UK's voice raises the possibility that EU data protection regulation could in future tilt towards privacy over security, or become less business-friendly. Professor Mitsilegas said it was "hard to predict the future",[205] but gave the example of the Data Retention Directive, which was pushed for by the UK only for it to be annulled after facing legal challenge from Digital Rights Ireland.[206] EU law was "rebalancing itself", and "different EU institutions are repositioning themselves", but this did not mean that future EU regulation would necessarily be "pro-privacy." He noted that Member States would still be likely to increase access to data for law enforcement purposes if they "perceive the population as being under threat."[207] Shona Riach, Europe Director at the Home Office, told us that "in all this debate there is always a balance to be struck between data protection and security, and the exact balancing point varies between Member States and, honestly, between different institutions in different Member States." She suggested that "recent events in Europe have moved the debate forward", and that

197 Q 67
198 Q 47
199 Q 47
200 Q 12 and Q 15
201 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119/132, 4 May 2016, pp 132–149)
202 Directive 2006/24/EC of the European Parliament and of the Council of 27 April 2016 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105/54, 13 April 2006, pp 54–63)
203 Q 15
204 Q 15
205 Q 15
206 Q 15. Directive 2006/24/EC was declared invalid by the Court of Justice of the European Union in April 2014 in the joined cases of *Digital Rights Ireland and Seitlinger and Others v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General* (2014) C-293/12 and C-594/12
207 Q 15

there was movement towards "a recognition" that "security of citizens is of paramount importance."[208]

147. Antony Walker suggested the UK could "still be at the forefront of the debate", but argued that to remain influential the UK Government would need to be "at the forefront of thinking" about how we get the balance right between protection of citizens' rights and security issues.[209] The Information Commissioner agreed that finding the right balance between privacy and security would be "difficult" and "challenging."[210] She noted that following recent terrorist attacks, there was a "deep recognition" among national data protection authorities of the need to balance these two areas.[211] She believed the UK had been "very influential" in emphasising that "it is not public safety or privacy, it is public safety and privacy … [it is] not a zero-sum game."[212] But like Professor Mitsilegas, she observed that "the courts are getting involved … more and more", and that "it is up to the courts to do some of that balancing."[213]

The European Data Protection Board

148. The ICO is the UK's independent data protection regulator (or national supervisory authority) and the main body through which the UK works with EU and other data protection authorities around the world. The ICO regulates both public and private sectors with the aim of safeguarding the privacy and data protection rights of the public and administering relevant laws.[214]

149. For as long as the UK remains a member of the EU, the UK's Information Commissioner will automatically be a member of the European Data Protection Board (EDPB) created by the GDPR.[215] The EDPB will replace the Article 29 Working Party, on which the national data protection authorities of the 28 EU Member States, the European Data Protection Supervisor (EDPS) and the European Commission are currently represented.[216]

150. The Information Commissioner predicted that the EDPB will have "a more powerful role" than the Article 29 Working Party, "primarily because a disagreement between supervisory authorities over how to deal with a particular matter can be resolved through a legally binding majority vote"—in contrast to the Article 29 Working Party, which serves as an advisory

208 Q 66
209 Q 47
210 Q 30
211 Q 37
212 Q 30
213 Q 30
214 See Q 22. The ICO administers the 1998 Data Protection Act, 2000 Freedom of Information Act and the Privacy and Electronic Communications Regulations.
215 Under Article 68(3), Regulation (EU) 2016/679 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, pp 1 –88) the EDPB is comprised of "the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives." See Chapter one for more information about the EDPB. Article 54(1)(b) of the 1998 Data Act states that the Information Commissioner will be the supervisory authority for the United Kingdom for the purposes of the Data Protection Directive and the Data Protection Framework.
216 The Article 29 Working Party is established by Article 29 of the 1995 Data Protection Directive. It provides the European Commission with independent advice on data protection matters and assists with the development and coordination of data protection policy across EU Member States.

body.[217] The EDPB will "adjudicate between national supervisory authorities over cases/investigations/complaints and will issue independent and binding decisions."[218] The Information Commissioner also drew attention to the EDPB's new powers to "make decisions about the data processing of companies and organisations that impact on UK citizens",[219] and its role in interpreting 'trigger terms' in the GDPR, suggesting that this was "why the ICO has been more active than ever as the Article 29 Working Party transforms into the EDPB."[220]

151. Only EU Member States' national data protection authorities will be members of the EDPB. It follows that once the UK leaves the EU, it will no longer be represented on the EDPB. The Information Commissioner told us that the ICO's relationship with the EDPB would "necessarily change",[221] and that it would be "very important" for the Government to consider how the ICO could continue to exert influence on the EDPB post-Brexit. She anticipated that the EDPB would "continue to be very influential in setting EU and international data protection standards", and noted that because of the "extra-territorial reach of the GDPR, the EDPB will have direct effect on UK businesses providing services to European citizens."[222] There was a risk therefore that the UK could find itself "outside, pressing our faces on the glass … without influence and yet have adopted fulsomely the GDPR."[223] She urged the Government to "do anything they can" to ensure that the ICO had "some status, be it observer status" or something similar, on the EDPB.[224] Failure to achieve this would be "frustrating for citizens and for Government."[225]

Oversight of Europol, Eurojust and EU data-sharing for law enforcement

152. In addition to its role on the EDPB, the ICO, as the national data protection authority of an EU Member State, plays a role in providing oversight of data protection by EU agencies and data-sharing platforms—a role that is also set to end once the UK leaves the EU.

153. Europol's operations are currently supervised by the Europol Joint Supervisory Body (JSB), which ensures it complies with data protection rules. The Europol JSB draws its membership from the national data protection authorities of the EU Member States, including the Information Commissioner's Office. Under the Europol Regulation[226] the European Data Protection Supervisor—an independent supervisory authority responsible for ensuring that EU institutions and bodies comply with EU data protection law when processing personal data—will take over responsibility from the JSB for the data protection supervision of Europol from 1 May 2017. The EDPS will provide advice on data protection issues to Europol and carry out inspections, as well as investigating complaints from individuals. The new

217 Written evidence from Elizabeth Denham (DPP0001)
218 Written evidence from Elizabeth Denham (DPP0001)
219 Q 26
220 Written evidence from Elizabeth Denham (DPP0001)
221 Written evidence from Elizabeth Denham (DPP0001)
222 Written evidence from Elizabeth Denham (DPP0001)
223 Q 29
224 Q 26
225 Q 26
226 Regulation 2016/794/EU of the European Parliament and the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135/53, 24 May 2016, pp 53–114)

Europol Regulation also sets up a new Cooperation Board comprising the EDPS and Members States' national supervisory authorities.

154. Eurojust has its own Joint Supervisory Body, established by Article 23 of the Eurojust Decision. The Euorojust JSB monitors Eurojust's activities where they involve the processing of personal data and ensures they are carried out in accordance with the Eurojust Decision.

155. The Information Commissioner told us that the ICO contributed to the "cooperative oversight" of Europol and Eurojust as well as the Schengen Information System (SIS II), to ensure that privacy and data protection rights of UK citizens "are respected." [227] She warned that the UK, as a third country post-Brexit, "will not have any oversight role" of any investigations and reviews conducted by the EDPS (or by the EDPS jointly with national supervisory authorities in the Member States) of "very sensitive data", including potentially the data of UK citizens.[228]

UK influence on regulation in other jurisdictions

156. Antony Walker judged that it was "an open question" whether the ICO would be able to gain observer or some other type of status on the EDPB post-Brexit, but he believed that the UK would still have "opportunities to influence" the EU by "talking to data protection authorities across Europe."[229] He proposed that such bilateral discussions should focus on the EU's largest economies, Germany, France, Spain and Italy, as well as "the economies that are at the forefront of digital innovation", such as the "Scandinavian countries and the Baltic States."[230]

157. Mr Walker also emphasised that for the UK to be on the "front foot" in such discussions would require a better funded and "more outward-looking ICO", able to "engage internationally."[231] He continued:

> "The ICO can be a very powerful advocate on an international stage. It can be an advocate for good practice in getting the balance of practical and pragmatic regulation right—regulation that means something and is not just words on a page … the ICO has an extremely important enabling role for business and for citizens, and an important role … to work with our counterparts internationally, and it needs the resources to be able to do that."[232]

158. The Information Commissioner told us that her office was "engaging in global enforcement work beyond Europe, to build bridges with other regulators around the world." She suggested that reaching out beyond Europe was important, "not just because of exiting the EU but because data knows no borders."[233] She noted that the ICO had the "ability in law" to conclude agreements with jurisdictions outside the EU "to cooperate and enforce

227 Q 23. See here for a more detailed description of the ICO supervisory role at an EU level: Information Commissioner's Office, 'International Duties': https://ico.org.uk/about-the-ico/what-we-do/international-duties [accessed 11 July 2017].
228 Q 23
229 Q 47
230 Q 47
231 Q 47
232 Q 52
233 Q 27

the law", and could also cooperate in "an investigation or data breach that involves several jurisdictions."[234]

159. Regarding the UK's global role in influencing data protection standards, the Information Commissioner identified the International Conference of Data Protection and Privacy Commissioners as "a really important forum", bringing together data protection authorities from around the world.[235] She also highlighted the network of Asia Pacific Privacy Authorities (of which the UK is not a member) and Common Thread, a network co-chaired by the UK and comprising Commonwealth member states.[236] Through Common Thread, the UK was working with Commonwealth countries to "raise the bar" on data protection laws, and "to work on consistency across the board."[237] When asked if the UK's influence was likely to change post-Brexit, she told us that while the UK would continue to "be involved" in these global fora, "the one I am worried about is the European Data Protection Board. It will be very influential."[238]

160. Stewart Room stressed that data protection issues were "not just a European and UK interest" but a matter of global concern.[239] The UK was "at the heart" of the Global Privacy Enforcement Network (GPEN), comprising regulatory authorities around the world including the EU (currently represented by the European Data Protection Supervisor) and the US Federal Trade Commission, and the UK had "led the development" of Common Thread.[240] Mr Room told us that these networks and fora "should give us confidence" that the UK would continue to "have influence behind the scenes and potentially at the sharp end of data protection."[241] Mr Room was also "sure" the UK would continue to have influence in Europe post-Brexit, adding that he did "not perceive any sense at all that the UK's skill and leadership are not valued" in the field of data protection, including in law enforcement.[242]

Prospect of an international treaty

161. In the longer term, the Information Commissioner told us that "there is now a great desire for more harmonisation and higher standards."[243] She noted that data protection laws were "converging more than they did", that international fora were "active", and that there was "much collaboration", demonstrating that data protection was no longer "a back-room, back-office, backburner issue."[244] Ms Denham predicted that "the end game, five or 10 years from now, probably needs to be an international treaty on data protection … It is on the horizon … that is where we need to go if we recognise the global nature of data flows."[245]

---

234 Q 27
235 Q 29
236 Q 29. See also The Common Thread Network, 'Homepage': https://commonthreadnetwork.org [accessed 11 April 2017].
237 Q 29
238 Q 29
239 Q 12
240 Q 13
241 Q 13
242 Q 15
243 Q 29
244 Q 29
245 Q 29

162. Antony Walker also saw the appeal of working on data protection at the global level, arguing that driving "a more harmonised approach internationally" would make it "easier for businesses to trade and means that consumers and citizens are confident and clear about the way in which their rights are protected."[246] He told us that, within the technology sector internationally, there was "a striking commonality of view", and that TechUK was keen to build relationships aimed at developing a "common international understanding across major markets about how we can create the kind of framework that our businesses and our citizens will need going forward."[247]

Conclusions and recommendations

163. **Even if the UK's data protection rules are aligned with the EU regime to the maximum extent possible at the point of Brexit, there remains the prospect that over time, the EU will amend or update its rules. Maintaining unhindered data flows with the EU post-Brexit could therefore require the UK to continue to align domestic data protection rules with EU rules that it no longer participates in setting.**

164. **Even if the Government does not pursue full regulatory equivalence in the form of an adequacy decision, the UK will retain an interest in the way the EU's regulatory framework for data protection develops. There is no prospect of a clean break: the extra-territorial reach of the GDPR means that the legal controls placed by the EU on transfers of personal data outside its territory will apply when data is transferred from the EU to the UK, affecting UK businesses that handle EU data.**

165. **The way that EU institutions such as the new European Data Protection Board and the Court of Justice of the European Union interpret the EU's data protection laws could also affect the UK, albeit indirectly—as demonstrated by the experience of the United States with Safe Harbour. Any changes to EU data protection laws would potentially alter the standards which the UK would need to meet to maintain an adequate level of protection. The UK could find itself held to a higher standard as a third country than as a Member State, since it will no longer be able to rely on the national security exemption in the TFEU that is currently engaged when the UK's data retention and surveillance regime is tested before the CJEU.**

166. **The UK has a track record of influencing EU rules on data protection and retention. Brexit means that it will lose the institutional platform from which it has been able to exert that influence. It is imperative that the Government considers how best to replace those structures and platforms in order to retain UK influence as far as possible. It should start by seeking to secure a continuing role for the Information Commissioner's Office on the European Data Protection Board.**

167. **In the longer term, it is conceivable that an international treaty on data protection could emerge as the end product of greater coordination between data protection authorities in the world's largest markets. The Government's long-term objective should be to influence the development of any such treaty. Given the relative size of the UK market compared to the EU and US markets, and its alignment with**

246 Q 47
247 Q 47

EU rules at the point of exit, the Government will need to work in partnership with the EU to achieve that goal—again underlining the need to adequately replace existing structures for policy coordination.

SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

1. The Government has said that it wishes to secure unhindered and uninterrupted flows of data between the UK and the EU post-Brexit, to facilitate both trade and law enforcement cooperation. We support this objective, and note that any arrangement that resulted in greater friction around data transfers between the UK and the EU post-Brexit could hinder police and security cooperation. It could also present a non-tariff barrier to trade, particularly in services, putting companies operating out of the UK at a competitive disadvantage. The Government must not only signal its commitment to unhindered and uninterrupted flows of data, but set out clearly, and as soon as possible, how it plans to deliver that outcome. We were struck by the lack of detail in the Government's assurances thus far. (Paragraph 110)

2. There was consensus among our witnesses that the most effective way to achieve unhindered flows of data would be to secure adequacy decisions from the European Commission under Article 45 of the General Data Protection Regulation and Article 36 of the Police and Criminal Justice Directive, thereby confirming that the UK's data protection rules offered an equivalent standard of protection to that available within the EU. (Paragraph 111)

3. Although other legal mechanisms to facilitate cross-border flows of data are available, we were persuaded by the Information Commissioner's view that the UK is so heavily integrated with the EU—three-quarters of the UK's cross-border data flows are with EU countries—that it would be difficult for the UK to get by without an adequacy arrangement. We therefore recommend that the Government should seek adequacy decisions to facilitate UK-EU data transfers after the UK has ceased to be a member of the EU. This would provide the least burdensome and most comprehensive platform for sharing data with the EU, and offer stability and certainty for businesses, particularly SMEs. (Paragraph 112)

4. Adequacy decisions can only be taken in respect of third countries, and there are therefore legal impediments to having such decisions in place at the moment of exit. In the absence of a transitional arrangement, this could put at risk the Government's objective of securing uninterrupted flows of data, creating a cliff-edge. We urge the Government to ensure that any transitional arrangements agreed during the withdrawal negotiations provide for continuity of data-sharing, pending the adoption of adequacy decisions in respect of the UK. (Paragraph 113)

5. In the absence of such transitional arrangements, the lack of tried and tested fall-back options for data-sharing in the area of law enforcement would raise concerns about the UK's ability to maintain deep police and security cooperation with the EU and its Member States in the immediate aftermath of Brexit. (Paragraph 114)

6. The need for transitional arrangements also extends to the commercial sector. Although there are alternative mechanisms to allow data to flow out of the EU for commercial purposes, these are sub-optimal compared to an adequacy decision, and may not be available to some types of companies, for instance small companies or those dealing directly with consumers. Some are also currently subject to legal challenge, notably the *Schrems II* case

against Standard Contractual Clauses, underlining the need for a transitional arrangement. (Paragraph 115)

7. The EU-US Privacy Shield and the EU-US Umbrella Agreement will cease to apply to the UK post-Brexit. Because of EU rules for onward transfers, securing unhindered flows of data with the EU may require the UK also to demonstrate that it has put arrangements in place with the US that afford the same level of protection as the Privacy Shield and the Umbrella Agreement. As regards data-sharing for commercial purposes, we note the approach taken by Switzerland, which has secured both an adequacy decision from the EU and a mirror of the Privacy Shield agreement with the US. (Paragraph 116)

8. Even if the UK's data protection rules are aligned with the EU regime to the maximum extent possible at the point of Brexit, there remains the prospect that over time, the EU will amend or update its rules. Maintaining unhindered data flows with the EU post-Brexit could therefore require the UK to continue to align domestic data protection rules with EU rules that it no longer participates in setting. (Paragraph 163)

9. Even if the Government does not pursue full regulatory equivalence in the form of an adequacy decision, the UK will retain an interest in the way the EU's regulatory framework for data protection develops. There is no prospect of a clean break: the extra-territorial reach of the GDPR means that the legal controls placed by the EU on transfers of personal data outside its territory will apply when data is transferred from the EU to the UK, affecting UK businesses that handle EU data. (Paragraph 164)

10. The way that EU institutions such as the new European Data Protection Board and the Court of Justice of the European Union interpret the EU's data protection laws could also affect the UK, albeit indirectly—as demonstrated by the experience of the United States with Safe Harbour. Any changes to EU data protection laws would potentially alter the standards which the UK would need to meet to maintain an adequate level of protection. The UK could find itself held to a higher standard as a third country than as a Member State, since it will no longer be able to rely on the national security exemption in the TFEU that is currently engaged when the UK's data retention and surveillance regime is tested before the CJEU. (Paragraph 165)

11. The UK has a track record of influencing EU rules on data protection and retention. Brexit means that it will lose the institutional platform from which it has been able to exert that influence. It is imperative that the Government considers how best to replace those structures and platforms in order to retain UK influence as far as possible. It should start by seeking to secure a continuing role for the Information Commissioner's Office on the European Data Protection Board. (Paragraph 166)

12. In the longer term, it is conceivable that an international treaty on data protection could emerge as the end product of greater coordination between data protection authorities in the world's largest markets. The Government's long-term objective should be to influence the development of any such treaty. Given the relative size of the UK market compared to the EU and US markets, and its alignment with EU rules at the point of exit, the Government will need to work in partnership with the EU to achieve that goal—again underlining the need to adequately replace existing structures for policy coordination. (Paragraph 167)

APPENDIX 1: LIST OF MEMBERS AND DECLARATIONS OF INTEREST

Members

Baroness Browning
Lord Condon
Lord Cormack (Member until 27 April 2017)
Lord Crisp
Baroness Janke
Lord Jay of Ewelme (Chairman)
Lord Kirkhope of Harrogate
Baroness Massey of Darwen
Lord O'Neill of Clackmannan
Baroness Pinnock
Baroness Prashar (Chairman until 27 April 2017)
Lord Ribeiro
Lord Soley
Lord Watts

Declaration of interests

Baroness Browning
No relevant interests declared

Lord Condon
No relevant interests declared

Lord Cormack
No relevant interests declared

Lord Crisp
No relevant interests declared

Baroness Janke
No relevant interests declared

Lord Jay of Ewelme
Member, Advisory Council, European Policy Forum
Member, Senior European Experts Group

Lord Kirkhope of Harrogate
Solicitor (England and Wales)
Member of European Parliament (1999–2016) (Conservative Spokesman on Justice and Home Affairs (2009–2016))

Baroness Massey of Darwen
No relevant interests declared

Lord O'Neill of Clackmannan
No relevant interests declared

Baroness Pinnock
No relevant interests declared

Baroness Prashar
No relevant interests declared

Lord Ribeiro
No relevant interests declared

Lord Soley
No relevant interests declared

Lord Watts
No relevant interests declared

The following Members of the European Union Select Committee attended the meeting at which the report was approved

Baroness Armstrong of Hill Top
Baroness Browning
Lord Cromwell
Lord Jay of Ewelme
Baroness Neville-Rolfe
Earl of Kinnoull
Lord Whitty
Baroness Wilcox
Lord Woolmer of Leeds
Baroness Verma

During consideration of the report the following Members declared an interest:

Baroness Neville-Rolfe

Minister of Data Protection (2015–16) as one of my ministerial responsibilities at the Department for Culture, Media and Sport

Commercial Secretary (Minister of State) at Her Majesty's Treasury (interest ceased 15 June 2017) (interest as Minister of State at the Department for Business, Energy and Industrial Strategy ceased 21 December 2016)

A full list of Members' interests can be found in the Register of Lords' Interests: http://www.parliament.uk/mps-lords-and-offices/standards-and-financial-interests/house-of-lords-commissioner-for-standards-/register-of-lords-interests/

APPENDIX 2: LIST OF WITNESSES

Evidence is published online at www.parliament.uk/brexit-eu-data-protection-package and available for inspection at the Parliamentary Archives (020 7219 3074).

Evidence received by the Committee is listed below in chronological order of oral evidence session and alphabetical order. Those witnesses marked with ** gave both oral and written evidence. Those marked with * gave oral evidence and did not submit written evidence. All other witnesses submitted written evidence only

List of witnesses in chronological order

*	Rt Hon. Matt Hancock MP	QQ 1–8
**	Stewart Room	QQ 9–21
*	Professor Valsamis Mitsilegas	
*	Rosemary Jay	
**	Elizabeth Denham	QQ 22–41
*	Anthony Walker	QQ 42–53
*	Ruth Boardman	
*	Baroness Williams of Trafford	QQ 54–68
*	Shona Riach	
*	Lucy Bird	

Alphabetical list of all witnesses

*	Lucy Bird	
*	Ruth Boardman	
**	Elizabeth Denham	DPP0001
*	Rt Hon. Matt Hancock MP	
*	Rosemary Jay	
*	Professor Valsamis Mitsilegas	
*	Shona Riach	
**	Stewart Room	DPP0002
*	Anthony Walker	
*	Baroness Williams of Trafford	

APPENDIX 3: GLOSSARY OF TERMS

BCRs	Binding Corporate Rules
CJEU	Court of Justice of the European Union
DRIPA	Data Retention and Investigatory Powers Act
ECRIS	European Criminal Records Information System
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
GDPR	General Data Protection Regulations
GPEN	Global Privacy Enforcement Networks
ICO	Information Commissioner's Office
JSB	Europol Joint Supervisory Body
PCJ	Police and Criminal Justice Directive, also known as the Law Enforcement Directive
SCCs	Standard Contractual Clauses
SIS II	Second Generation Schengen Information System
SMEs	Small and Medium Enterprises
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TPP	Trans-Pacific Partnership