Author: Simon McGarr, Data Compliance Europe

9 August 2019

Personal Data Transfers After Brexit

An Analysis Paper

(Updated: Aug 2019)

12 Citygate

Lower Bridge Street

Dublin 8

https://datacomplianceeurope.eu

Table of Contents

Appendices

1. Schrems Judgement on Safe Harbour
2. Brexit and Data Transfers Oxford University paper
3. UK DEXEU Report: Legislating for the
4. UK withdrawal from the EU
5. House of Lords Report on Brexit and personal data
6. UK Parliament paper- The exchange and protection of personal data

8. EU Position paper on the Use of Data and Protection of Information Obtained or Processed before the withdrawal date
9. EU Commission Notice to Stakeholders on Data Transfers
10. EDPS: Note on Personal Data Transfers After Brexit

Scope

Data Compliance Europe has undertaken this analysis of the potential effects on transfers of personal data arising from the United Kingdom of Great Britain and Northern Ireland's (UK hereafter) planned departure from the European Union, a process colloquially known as Brexit.

The focus of this analysis is the effect of Brexit on the flow of personal data between EU-based companies and both their UK partner companies and the cloud providers of services to EU companies, such as Salesforce.

This analysis is grounded in the ongoing analysis project being undertaken by Data Compliance Europe to ensure its client organisations are compliant with the General Data Protection Regulation. It is not intended to address each and every potential cross-border data transfer individually, but rather to address the issues of principle which will apply to them all.

By definition, the Brexit process is a novel and continuously developing legal and political situation. However, while all elements of this report are subject to changes in the circumstances of Brexit, we have attempted to address the most likely outcomes to the best of our ability at the time of writing, and to demonstrate the basis of our analysis with reference to the known facts.

Following the principles of John Maynard Keynes, if the facts were to change we expect that our analysis and conclusions would do so also.

Aug 2019

Description of Circumstances

On the 23rd June 2016, the UK voted in an advisory, non-binding referendum to leave the European Union. It was not immediately clear what the consequences of this vote would be for the UK's relationship with the EU. Many potential outcomes from that vote were politically extinguished on the 2nd October 2016 when the UK Prime Minister, Ms. Theresa May announced to the Conservative Party conference that her government;

1) Intended to trigger Article 50 no later than March 2017[1]
2) That the UK intended to take any steps necessary to remove itself from the jurisdiction of the Court of Justice of the European Union[2].
3) That the UK would seek to repeal existing EU law (the acquis) and then incorporate the same laws, with a UK legislative basis.[3]

The cumulative effect of these political decisions has seen the UK commence the process of leaving the EU in March 2017, with a consequent initial departure date set in law of 29th March 2019. That date was extended on application of the UK by a unanimous decision of the other 27 EU member states to the 31st October 2019.

Negotiations between the EU and the UK resulted in the terms of a Withdrawal Agreement on the UK's departure terms being settled between the UK Government and the EU27. However, despite presenting this Withdrawal Agreement to the UK parliament three times,

---

1. "We will invoke Article Fifty no later than the end of March next year." http://press.conservatives.com/post/151239411635/prime-minister-britain-after-brexit-a-vision-of
2. "Our laws will be made not in Brussels but in Westminster. The judges interpreting those laws will sit not in Luxembourg but in courts in this country. The authority of EU law in Britain will end." *ibid*
3. "As we repeal the European Communities Act, we will convert the 'acquis' – that is, the body of existing EU law – into British law" *ibid*

Mrs. May was unable to muster sufficient votes to have it accepted by the legislature.

The EU has said that it will not reopen the negotiations on the Withdrawal Agreement. Mrs. May's replacement as Prime Minister, Mr. Boris Johnson has stated that he will refuse to open discussions with the EU unless it preemptively agrees to amend the Withdrawal Agreement.

If matters stay unchanged. the UK will leave the EU on 31st October 2019 without any agreement addressing its relationship with the EU. We will term this scenario the "Chaotic Hard Brexit".

An alternative situation will be that the UK succeeds in obtaining agreement from the EU27 to some mutually acceptable deal and then succeeds in concluding a trade agreement with the EU, all in advance of the October 2019 departure deadline, in line with its current declared policies. We will term this scenario the "Orderly Hard Brexit".

These two scenarios will be addressed as the main possibilities facing EU business. However, it would be remiss, given the very volatile and unpredictable nature of these matters, not to also outline the less likely alternatives. The first of these would see a reversal of the policy positions adopted in the former Prime Minister's speech of the 2nd October 2016. This would allow the UK to depart the EU, but to accept the continuing authority of the CJEU and recognise the effect of the Charter of Fundamental Rights. This would allow the UK to remain in the Single Market and/or the Customs Union. We will term this scenario the "Soft Brexit".

Finally, there remains the possibility that the UK could seek to withdraw its triggering of Article 50 of the Treaty on the Functioning of the European Union, remaining a member of the EU. We will term this scenario "No Brexit".

Before providing an analysis of the consequences of each of those scenarios, it is important to address the underlying legal position on data protection laws and the laws governing the transfer of personal data common to them all. We will then examine the consequences of that legal framework for the UK.

EU Laws governing personal data transfers

The protection of personal data of EU residents has been an EU-wide legal requirement since the coming into force of the Data Protection Directive[4] on the 13th December 1995. The right to the protection of personal data was recognised by Article 8 of the Charter of Fundamental Rights[5] as one of the bedrock personal rights enshrined in EU law as part of the Treaty of Lisbon.[6] The General Data Protection Regulation[7] (the GDPR) further strengthens the framework for recognition and enforcement of that Fundamental Right.

EU member states may transfer personal data to other member states freely. It is accepted that, by virtue of their shared acceptance of the above legislative and Treaty framework, that they provide an adequate level of protection for personal data.

This has allowed the deep integration of intra-member data sharing into the EU economy. For the purposes of EU law, it is immaterial whether the personal data of one member state's citizens is stored in a data centre in another member state, as they are all deemed to share the same legal rights and enforcement framework.

However, the same level of protection cannot be taken as a given when it comes to transferring personal data to states outside the EU. To avail of similar seamless data transfers each state receiving EU personal data must demonstrate that they have an 'adequate' level of protections and

4. Directive 95/46/EC of the European Parliament and of the Council
5. http://www.europarl.europa.eu/charter/pdf/text_en.pdf
6. The Treaty on the Functioning of the European Union http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12007L/TXT&from=en
7. Regulation (EU) 2016/679 of the European Parliament of 27 April 2016 on the protection of natural persons with regard to the processing of per- sonal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Art 68(3), OJ 2016 L 119/1

enforcement, equivalent (even if not identical in form) to the EU's own protections. This examination extends to assessing the treatment of data in a national security context.

The alternative is to engage one of the existing transfer mechanisms covering transfers to third parties outside the EU, who must agree to impose upon themselves adequate protections on the data they receive.

The seriousness with which the EU takes this requirement was demonstrated in the *Schrems*[8] case, where a challenge brought before the Irish High Court was referred to the CJEU in Luxembourg, resulting in the CJEU striking down the finding of adequacy which underpinned a significant volume of all data transfers between the EU and the US. (The Safe Harbour Agreement)

In the *Schrems* judgement the CJEU stressed the significant tests[9] which must be met by any non-member state if the EU Commission is to legitimately issue a finding of adequacy. They also stated that it was a requirement that the Commission continually keep these decisions under review, and to revisit them in the light of any new information which comes to light. Since the GDPR comes into force, the group of EU data protection authorities, the European Data Protection Board, has also been given a duty to issue opinions on proposed adequacy decisions to be made by the EU Commission.

This is critical in the context of Brexit, as it means that **the issue of the adequacy of protections for data transfers to the EU cannot be definitively dealt with in the context of the UK's Brexit negotiations**.

---

8. Case C-362/14
Maximillian Schrems v Data Protection Commissioner
https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf
9. Articles 44-50, Regulation (EU) 2016/679 of the European Parliament 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), Art 68(3), OJ 2016 L 119/1

Even in the event that the UK were to obtain an adequacy decision from the EU Commission as part of their departure discussions, that finding would remain subject to CJEU challenge and to reversal by the EU Commission in the light of new information.[10]

This will leave companies with the option of either relying upon the alternative methods of transferring personal data to Third Party countries or on 'derogations'.

10. Article 45(5), Regulation (EU) 2016/679 of the European Parliament 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), Art 68(3), OJ 2016 L 119/1

Alternative methods of transferring data to Third Party countries

There are longstanding methods of transferring personal data for processing to entities in third countries. However, none of these systems are as seamless as a transfer between member states. At heart, this is because a Third Party country is presumed to start from a position of providing inadequate protections for personal data, while member states, by definition, provide all the protections of EU law.

For any body or organisation intending to continue to transfer EU data to the UK after Brexit has occurred, it is critical that it examine its options and commence preparation for adoption of one or more of these methods. None of them will be effortless, and most of them will require engagement with external data controllers and/or processors to ensure that, for example, contracts are altered or amended now to allow for the EU's standard contract clauses are incorporated.

The EU Commission has set out[11] four systems of 'appropriate safeguards" allowed for under the GDPR;

1. Standard data protection clauses: the Commission has adopted three sets of model clauses which are available on the Commission's website;
2. Binding corporate rules: legally binding data protection rules approved by the competent data protection authority which apply within a corporate group;
3. Approved Codes of Conduct together with binding and enforceable commitments of the controller or processor in the third country;
4. Approved certification mechanisms together with binding and enforceable commitments of the controller or processor in the third country.

11. http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245

Of the four methods above, 2 is burdensome and limited to transfers between parts of a single cross-border entity while 3 and 4 are largely unavailable. No Codes of Conduct[12] have yet to be approved, and no approved GDPR Certification mechanisms[13] have yet to emerge.

Transfers can also be made under the 'derogations', allowing transfers in specific cases. These largely track the legal basis clauses of Article 6 of the GDPR- on foot of consent, to perform a contract, to exercise legal claims or for public interest reasons. These will all require a considerable degree of preparation before they may be relied upon, to ensure, for example that any consent is sufficiently informed to be considered valid.

This leaves Standard Contract Clauses as the primary method of transferring EU-located personal data to Third Party countries for processing. This is a set of pre-written contractual clauses issued by the EU Commission, which can be incorporated into existing contracts by agreement on both sides.

While this system has permitted transfers between the EU and the US, there is a challenge taken by the Data Protection Commission of Ireland to the validity of that transfer model currently before the Irish Supreme Court, which may yet reach the CJEU.

If companies are to rely on Standard Contract Clauses after October 2019 for transfers of EU personal data to the UK, **it is imperative that preparatory action to allow for that commences now.**

12. https://edpb.europa.eu/our-work-tools/our-documents/topic/code-conduct_en

13. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_1_2018_certification_en.pdf

Challenges to a finding of adequacy for the UK

The UK government has suggested that the issue of data transfers will be neither contentious nor complicated following Brexit. In testimony to the House of Lords in February 2017, Mr. Matt Hancock MP, for the UK Government, set out their intention;

> "Our goals are clear. We want an arrangement that provides for the unhindered exchange of data, within an appropriate data protection environment….Not only do we seek unhindered data flows but we want that to happen in an uninterrupted way—that is to say, on the morning on which we have left the European Union"[14]

However, when asked, for example who the UK saw as the ultimate arbiter of such matters, if they were to leave the jurisdiction of the CJEU, Mr. Hancock acknowledged "We do not have the answer to that question, because we have not begun the negotiations, let alone concluded them."

The Minister of State at the Home Office, Baroness Williams asserted that "the UK will enjoy a unique position as a third country, given that, unlike other non-EU countries, it will have fully implemented EU [data] privacy rules.[15]

While the aims of the UK government are clear, the Baroness' assertion appears at variance with the legislative and legal facts. The UK's

---

14. https://www.parliament.uk/business/committees/committees-a-z/lords-select/eu-home-affairs-subcommittee/news-parliament-2015/minister-questioned-data-protection/

15. Baroness Williams of Trafford, evidence to the EU Home Affairs Sub-Committee, 26 April 2017 <http://parliamentlive.tv/Event/Index/ ed6b1fe1-c786-4768-9e63-a65b994cc8d7> 11:08:17–11:08:24

implementation of EU data privacy rules are currently under direct challenge, following both the Digital Rights Ireland[16] and Tele2[17] judgements from the CJEU. In addition, it is the intention of the UK to only partially transpose EU law into UK law.

Insofar as any solid implementation has been outlined, the text of the Data Protection Directive (and subsequently the GDPR) is proposed to be incorporated into UK law by way of an Act of Parliament, it is explicitly intended to omit the transposition of Article 8 of the Charter of Fundamental Rights on Brexit. This proposal was passed by a vote of the UK Parliament on the 21st November 2017.
The UK Government has set out its rationale for this policy:

> "It cannot be right that the Charter could be used to bring challenges against the Government, or for UK legislation after our withdrawal to be struck down on the basis of the Charter. On that basis the Charter will not be converted into UK law by the Great Repeal Bill."[18]

Article 8 of the Charter, which underpins the EU's Data Protection framework, has no equivalent in UK law. The UK has no written constitution and so any domestic statutory provision is always going to be distinctly different in character from the EU's Charter's Fundamental rights regime. A domestic UK law is subject to repeal or alteration by any Parliament.

---

16. Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, Intervener: Irish Human Rights Commission, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&from=EN
17. Tele2 Sverige AB (C-203/15) v Post-och telestyrelsen, and Secretary of State for the Home Office (C-698/15) v Tom Watson, Peter Brice, Geoffrey Lewis, interveners: Open Rights Group, Privacy International, The Law Society of England and Wales, http://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=EN
18. Department for Exiting the European Union, Legislating for the United Kingdom's Withdrawal from the European Union, Cm 9446, March 2017: [2.23]

In his Article "Data Transfers between the UK and the UK post Brexit?" in the Journal of *International Data Privacy Law*[19] Andrew D. Murray focussed on the critical gap this opens up between Data Protection rights in the UK, post-Brexit and those in the EU.

> "As Advocate General Jaaskinen demonstrated in *Google Spain SL and another v Agencia Espanola de Proteccion de Datos and another*,[20] there is a clear legal distinction between the Charter Rights and the Directive (or Regulation) which gives effect to them.
>
> "According to the ECHR and the Charter any interference to protected rights must be based on law and be necessary in a democratic society. In the present case we are not faced with interference by public authorities in need of justification but of the question of the extent that interference by private subjects can be tolerated. The limits to this are set out in the Directive, and they are thus based on law, as required by the ECHR and the Charter. Hence, when the Directive is interpreted, the exercise precisely concerns the interpretation of the limits set to data processing by private subjects in light of the Charter."[21]
>
> As will be argued below, this matters. There will no longer be a fundamental right to data protection in the UK post Brexit and this is something which cannot be remedied through domestic legal settlements short of a British Bill of Rights, and even then perhaps not so if Parliament retains sovereignty to amend or repeal these rights by normal Parliamentary procedures."[22]

---

19. Andrew D. Murray; Data transfers between the EU and UK post Brexit?, *International Data Privacy Law*, Volume 7, Issue 3, 1 August 2017, Pages 149–164, https://doi.org/10.1093/idpl/ipx015
20. Case C-131/12, 13 May 2014 ECLI:EU:C 2014:317 (Judgment) both reported at [2014] 3 CMLR 50.
21. Ibid [AG119] (emphasis added).
22. Andrew D. Murray; Data transfers between the EU and UK post Brexit?, *International Data Privacy Law*, Volume 7, Issue 3, 1 August 2017, Pages 151-152, https://doi.org/10.1093/idpl/ipx015

It is this change in the architecture of legal protections which, even if the UK's intention was to implement the GDPR in its entirety in UK legislation, represents the most significant breach in the equivalence between the post-Brexit UK and the EU in the framework of Data Protection rights protection.

UK Courts have made significant findings on Data Protection rights explicitly grounded on the Article 8 rights granted by the Charter (most famously on the right to compensation in *Vidal-Hall v Google*)[23]. These rights are not limited to the protection of data. They also include freestanding rights to seek reference to an independent data protection authority in the event of breach of those rights. The EU Commission has taken a number of successful cases to the CJEU against Member States, arguing that the provisions of implementing domestic legislation of local Data Protection Authorities falls short of the independence required under the Charter. (*Commission v Germany*,[24] *Commission v Austria*,[25] *Commission v Hungary*)[26]. The UK's current proposal will see those protections which underpins the Information Commissioner's Office (the UK's Data Protection Authority) removed and not replaced. Independence of the ICO will cease to be a matter of fundamental right and will be subject to any legislative changes the UK Government passes through Parliament.

The primary immediate obstacles to a finding of adequacy, however, may not be these constitutional and legal gaps. The most immediate challenges to a finding of adequacy stem from the UK's legislation in the areas of communication retention and mass surveillance. Specifically, the UK Investigatory Powers Act is, on its face and as a matter of stated UK policy, in direct conflict with Article 8 of the Charter of Fundamental Rights and the GDPR (as interpreted by the the CJEU in the *Digital*

23. Vidal-Hall v Google Inc (CA) [2015] EWCA Civ 311
24. C-518/07, Commission v. Germany
25. C-614/10, EU Commission V. Austria
26. C-288/12, EU Commission V. hungary

Rights Ireland v Ireland [27] and *Tele2* [28] cases)

Each of these cases set out the general principle that the mass surveillance of persons is a breach of Article 8 of the EU Charter and of the Data Retention Directive. Both then set out requirements which would have to be met to justify such a breach, including the nature of the threat to another right which was being affected, (limited to, for example, combating serious crime), and the safeguards which would have to be in place to oversee and limit impinging on citizens' personal rights to only that which was both necessary and proportionate.

In contrast Section 87(1) of the Investigatory Powers Act 2016 has a list of purposes for which data may be retained under UK law, and vests the power to determine proportionality and necessity in the Secretary of State and not the UK courts. The grounds go far beyond what is permitted under the CJEU's standards, and where it does address the prevention and detection of crime, it does not limit itself to serious crime.

In addition, it restricts the powers of the UK Data Protection Authority in respect of the data retention regime to one of mere data security audits, and does not allow for personal complaints to be addressed, as required under Article 8 of the Charter. Read in the light of the *Schrems* judgement that 'legislation to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification nor erasure of such data, does not respect the essence of the fundamental right to effective judicial protection as enshrined in Article 47 of the Charter' this seems to be a further significant point of divergence between the UK and EU legal positions.

By itself, this Act will pose a profound challenge to any effort to agree that the UK meets the standard of adequacy- involving, as it does, the

27. Joined Cases C–203/15 and C–698/15, 21 December 2016, ECLI:EU:C:2016:970

28. Tele2 Sverige AB v Post-och telestyrelsen (C–203/15) and Secretary of State for the Home Office v Tom Watson (C–698/15)

mass surveillance of the entire population of the UK.

The German MEP Jan Philipp Albrecht, at the time the rapporteur for data protection matters for the European Parliament's relevant committee and now a member of the German government, has set out his analysis of the situation in a pithy pair of tweet-sized statements.

> "Of course the UK will need an adequacy decision by the COM to not mess up data transfers with EU. But it will be almost impossible to grant[29].
> "Main reason: COM has to not only judge all data protection provisions but then (different than inside the EU) also national security rules."[30]

The UK government has demonstrated that they understand the risks these looming threats to data flows pose to their economy, which relies heavily on trade in international services.

In a speech made in March 2018, the UK Prime Minister, Ms. May, highlighted the issue of data transfers as one which the UK particularly wanted to reach an agreement, which would be 'more' than any arrangement previously made.

> [T]he free flow of data is also critical for both sides in any modern trading relationship too. The U.K. has exceptionally high standards of data protection. And we want to secure an agreement with the EU that provides the stability and confidence for EU and U.K. individuals and businesses to achieve our aims in maintaining and developing the U.K.'s strong trading and economic links with the EU.
>
> That is why we will be seeking more than just an adequacy arrangement and want to see an appropriate ongoing role for the UK's Information

29. @JanAlbreacht, 15th March 2017, https://twitter.com/JanAlbrecht/status/841984400476774400
30. @JanAlbreacht, 15th March 2017, https://twitter.com/JanAlbrecht/status/841986282238664704

> Commissioner's Office. This will ensure UK businesses are effectively represented under the EU's new 'one stop shop' mechanism for resolving data protection disputes.[31]

The response, most recently in May 2018, from M. Barnier for the EU27 acknowledges the role data flows have in the EU, but was as clear as could be that Ms. May's wish for something 'more' than adequacy was not something the EU was willing to concede.

> The United Kingdom needs to face up to the reality of the European Union. It also needs to face up to the reality of Brexit.
>
> The United Kingdom decided to leave our harmonised system of decision-making and enforcement.
>
> It must respect the fact that the European Union will continue to work on the basis of this system, which has allowed us to build a single market, and which allows us to deepen our single market in response to new challenges.
>
> And, as indicated in the European Council guidelines, the UK must understand that the only possibility for the EU to protect personal data is through an adequacy decision.[32]

31. https://www.bbc.com/news/uk-politics-43256183
32. http://europa.eu/rapid/press-release_SPEECH-18-3962_en.htm

The Withdrawal Agreement

On 14th November 2018, the EU and British Government published a draft of a withdrawal agreement to deal with the UK's departure from the EU.

The Agreement has since been endorsed by the governments of the EU member states. It has been rejected in three separate votes by the UK parliament.

It originally proposed the UK departure from the EU in March 2019, with a 'transition period' ending (initially) on the 31st December 2020. The departure date has since been extended to 31st October 2019. After that point the UK is bound to follow EU rules if it wishes to continue access to the EU (or, alternatively, to accept goods checks etc between Northern Ireland and the rest of the UK). This is secured by the 'backstop' mechanism.

For our purposes, the articles of primary interest in the Draft Withdrawal Agreement are Articles 127-129, dealing with the application of EU law during the Transition Period and Articles 70-73. These latter provisions deal with "Data and Information processed or obtained before the end of the transition period or on the basis of this agreement".

Article 71.1 confirms that EU law is applicable, directly in the UK, to data transfers made to countries outside the UK.
Article 71.2 says that EU law shall not directly apply in the UK to data processed under an adequacy decision.
Article 71.3 says that if there's no adequacy agreement the UK is bound to the requirement to provide the equivalent level of protection to data subjects as required under EU law.

Article 72 says that EU data law will apply to the organs of the UK state.

Article 73 says that UK data which is transferred to the EU shall be treated as though it were the data of a Member State. It does not say

that the converse is also true.

This has been read- insofar as any public attention has been paid to the issue- as meaning that the UK may carry on as before and be treated as if it were a member state for the purposes of data transfers during the Transition period.

This is clearly not stated in Articles 70-73, on data processing.

The source of this misunderstanding can be found in a misreading of Article 127.1 and 127.3, read together.

Art 127.1:

> Unless otherwise provided in this Agreement, Union law shall be applicable to and in the United Kingdom during the transition period.

Art 127.3

> During the transition period, the Union law applicable pursuant to paragraph 1 shall produce in respect of and in the United Kingdom the same legal effects as those which it produces within the Union and its Member States, and shall be interpreted and applied in accordance with the same methods and general principles as those applicable within the Union.

The problem is that Union law is clear about one thing- that transferring personal data to a non-Member state requires a legal basis. Article 73 says that UK data which is transferred to the EU shall be treated as though it were the data of a Member State.

It carefully does not say that EU data transferred to the UK shall be considered to be travelling to a Member State. It cannot, because the EU negotiations can't agree something that would be illegal under EU law.

European Union law is agreed to have the same 'legal effects' as those which it produces in the Union and its Member states, under Article 127.3. But, within the Union and its Member states, the effects of a

personal data transfer under Union law depend on whether the destination country is a Member state, or whether it is not.

After October 2019, the UK will not be a Member state. And the agreement to apply Union law will have the legal effects which flow from that fact.

Consequences of four possible Brexit outcomes

Chaotic Hard Brexit

This is currently the most likely outcome. If the UK reaches the deadline of the 31st October 2019 without having completed an agreement on the terms of its departure from the EU with the other 27 members, it will automatically cease to be a member on that date.

The consequences of such an outcome would be immediately severe and disruptive in many fields of activity (UK would lose the benefit of the Open Skies agreement allowing EU aeroplanes access to UK airspace, to give one dramatic example[33]). However, we will limit our consideration to the consequences for data transfers.

The UK will have become a Third Country for the purposes of the GDPR overnight. It will have no Article 45 adequacy agreement in place, and no prospect of obtaining one for an unknown length of time, even if its laws had been brought into line with the EU's system. (The Privacy Shield agreement on data transfers with the US was the outcome of approximately 2 years of negotiations and is significantly more restricted than a full adequacy finding under Article 45).

The UK's Data Protection Act, seeking to implement GDPR rules in a UK legislative framework, will lose the underpinnings of the Charter of Fundemental Rights. Article 46 of the GDPR allows for international transfers subject to individual data controllers and processors giving undertakings that the jurisdiction they're sending the data to meets the requirements of legal protections and effective legal remedies. It seems unlikely for individual Data Controllers to be able to provide such assurances. Article 47 of the GDPR allows for the use of Binding

33. http://www.telegraph.co.uk/news/2017/07/11/ryanair-chief-michael-oleary-discuss-brexit-effect-aviation/

Corporate Rules as a basis for transfer between bodies within a single organisation.

Given the terms of the Investigatory Powers Act, any transfer relying on Standard Contract Clauses may eventually run into the same difficulties as those which were identified in the *Schrems* case.

The result would be no obvious legal mechanism outside the limited 'derogations' which would allow for generalised transfer of EU personal data to the UK for an unknown period of time.

Orderly Hard Brexit

The UK leaves the EU on the 31st October 2019 having accepted the terms of the Withdrawal Agreement with the remaining EU27. The terms of that proposed agreement[34] are currently available and Article 63 of that agreement includes that the GDPR would continue to apply to the UK. That article is one which has already been agreed between the UK and EU27; however it is clear from the UK Government statements that they are seeking an adequacy finding as part of their post-transition deal, and that they want its provisions to go further and be more comprehensive than the withdrawal agreement.

However, for the reasons set out above and summarised by Mr. Albreacht MEP in his tweets[35], it will be very difficult for the UK to make

---

34. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759019/25_November_Agreement_on_the_withdrawal_of_the_United_Kingdom_of_Great_Britain_and_Northern_Ireland_from_the_European_Union_and_the_European_Atomic_Energy_Community.pdf

35. @JanAlbreacht, 15th March 2017, https://twitter.com/JanAlbrecht/status/841984400476774400

and

@JanAlbreacht, 15th March 2017, https://twitter.com/JanAlbrecht/status/841986282238664704

the transition from member state to Third Party with their legislation as it currently stands. The Investigatory Powers Act 2016 stands out as an effective block to any finding of adequacy in line with the CJEU's caselaw. The EU Commission may not act illegally, and it is difficult to see any finding of adequacy made under Article 45 standing without immediate challenge to the CJEU were they to do so.

On balance, as matters currently stand, it is more likely than not that there would not be a legal mechanism which would allow for generalised EU personal data unless and until the UK adjusts its current surveillance regime.

Soft Brexit

In this scenario, the UK leaves the EU, either on the 29th March 2019 or at a later date mutually agreed with the EU27. It abandons the current UK government policy of removing itself from the jurisdiction of the CJEU. It remains within the EEA, Single Market and/or the Custom Union. It incorporates the Charter of Fundamental Rights into its own law by way of the proposed British Bill of Rights or by reference to the Charter itself in domestic statutes. It repeals or amends the Regulatory Powers Act 2016 to bring it in line with the CJEU decisions in *Tele2* and *Digital Rights Ireland*.

The European Commission faces no political resistance or legal impediment to making a finding of adequacy congruent with the departure of the UK from the EU.

Under this scenario, there would therefore be no interruption in EU data transfers to the UK.

No Brexit

Article 50 of the TFEU permits for the triggering of notice of departure to be revoked by mutual agreement between the UK and the EU27.

Politically the EU27's representatives have made it clear that if the UK sought to revoke their triggering of Article 50 that they would be happy to see the UK remain in the EU,

Currently, this appears the most unlikely outcome of all those explored in this paper. However, for this outcome to occur would require nothing other than a political decision. As the events of the last two years have demonstrated, the possibility of unexpected political events occurring should not be discounted.

In the event that Brexit did not happen, there would be no change to the current data transfer regime to the UK.

Conclusions for Companies

The two most likely outcomes for Brexit (Chaotic or Orderly Hard Brexit) will both involve a high risk of interruption to lawful EU personal data transfers to the UK. This is particularly the case if the Chaotic Hard Brexit scenario unfolds.

The UK government's inability to explain how their stated aim of an interrupted data flow could be obtained reflects the difficulties in finding a way the EU could agree a legal mechanism to give that aim reality. Even an Orderly Hard Brexit seems more likely than not to result in significant barriers to data transfers.

For this reason, we are recommending that companies start a review of their data processing habits, to prepare for whichever Brexit outcome emerges. This should prompt companies to;

1. Engage with their data processors to ensure, wherever practical or possible, that the EU personal data they have responsibility for is stored and processed in an EU27 member state.
2. Examine the requirement for, and basis of, any and all personal data transfers to UK companies with a view to identifying where that data can instead be prepared solely in an aggregate, non-personally identifying manner wherever required, or otherwise irrevocably anonymised.
3. Identify EU-located data processing services to replace all of the services currently exclusively provided in the UK.
4. Where EU personal data will continue to be transferred to the UK, immediately start the process of identifying those data flows and put in place alternative legal data transfer mechanisms to allow them to continue after Brexit, such as Standard Contract Clauses agreements or the use of Binding Contract Terms.
5. Consider if companies operating on an all-island of Ireland basis

can integrate personal data from Northern Ireland into their systems in such a way as to ensure that no personal data from the EU residents are transferred to any location in Northern Ireland.

Works Cited

Andrew D. Murray; Data transfers between the EU and UK post Brexit?, *International Data Privacy Law*, Volume 7, Issue 3, 1 August 2017, Pages 149–164, https://doi.org/10.1093/idpl/ipx015

HOUSE OF LORDS European Union Committee, Brexit: the EU data protection package, 3rd Report of Session 2017–19, HL Paper 7

HM Government, The exchange and protection of personal data, 2017 (Cm)

Department for Exiting the European Union, Legislating for the United Kingdom's Withdrawal from the European Union, Cm 9446

Conservative Party Conference Speech, Theresa May, 2nd October 2016, http://press.conservatives.com/post/151239411635/prime-minister-britain-after-brexit-a-vision-of

Directive 95/46/EC of the European Parliament and of the Council

Regulation (EU) 2016/679 of the European Parliament

Charter of Fundamental Rights of the European Union, Treaty of Lisbon http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12007L/TXT&from=en

The Telegraph, *Ryanair boss: 'No flights' between UK and EU after Brexit,* 11th July 2017

Appendix 1:

CJEU Judgement

Data Protection Commissioner v Schrems and Joined Party Digital Rights Ireland, Case C-362/14

Reports of Cases

JUDGMENT OF THE COURT (Grand Chamber)

6 October 2015 *

(Reference for a preliminary ruling — Personal data — Protection of individuals with regard to the processing of such data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Directive 95/46/EC — Articles 25 and 28 — Transfer of personal data to third countries — Decision 2000/520/EC — Transfer of personal data to the United States — Inadequate level of protection — Validity — Complaint by an individual whose data has been transferred from the European Union to the United States — Powers of the national supervisory authorities)

In Case C-362/14,

REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014, in the proceedings

Maximillian Schrems

v

Data Protection Commissioner,

joined party:

Digital Rights Ireland Ltd,

THE COURT (Grand Chamber),

composed of V. Skouris, President, K. Lenaerts, Vice-President, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), S. Rodin and K. Jürimäe, Presidents of Chambers, A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský, D. Šváby, M. Berger, F. Biltgen and C. Lycourgos, Judges,

Advocate General: Y. Bot,

Registrar: L. Hewlett, Principal Administrator,

having regard to the written procedure and further to the hearing on 24 March 2015,

after considering the observations submitted on behalf of:

— Mr Schrems, by N. Travers, Senior Counsel, P. O'Shea, Barrister-at-Law, G. Rudden, Solicitor, and H. Hofmann, Rechtsanwalt,

— the Data Protection Commissioner, by P. McDermott, Barrister-at-Law, S. More O'Ferrall and D. Young, Solicitors,

* Language of the case: English.

— Digital Rights Ireland Ltd, by F. Crehan, Barrister-at-Law, and S. McGarr and E. McGarr, Solicitors,

— Ireland, by A. Joyce, B. Counihan and E. Creedon, acting as Agents, and D. Fennelly, Barrister-at-Law,

— the Belgian Government, by J.-C. Halleux and C. Pochet, acting as Agents,

— the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,

— the Italian Government, by G. Palmieri, acting as Agent, and P. Gentili, avvocato dello Stato,

— the Austrian Government, by G. Hesse and G. Kunnert, acting as Agents,

— the Polish Government, by M. Kamejsza, M. Pawlicka and B. Majczyna, acting as Agents,

— the Slovenian Government, by A. Grum and V. Klemenc, acting as Agents,

— the United Kingdom Government, by L. Christie and J. Beeko, acting as Agents, and J. Holmes, Barrister,

— the European Parliament, by D. Moore, A. Caiola and M. Pencheva, acting as Agents,

— the European Commission, by B. Schima, B. Martenczuk, B. Smulders and J. Vondung, acting as Agents,

— the European Data Protection Supervisor (EDPS), by C. Docksey, A. Buchta and V. Pérez Asinari, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 23 September 2015,

gives the following

Judgment

1 This request for a preliminary ruling relates to the interpretation, in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union ('the Charter'), of Articles 25(6) and 28 of 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 1995 L 281, p. 31), as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003 (OJ 2003 L 284, p. 1) ('Directive 95/46'), and, in essence, to the validity of Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7).

2 The request has been made in proceedings between Mr Schrems and the Data Protection Commissioner ('the Commissioner') concerning the latter's refusal to investigate a complaint made by Mr Schrems regarding the fact that Facebook Ireland Ltd ('Facebook Ireland') transfers the personal data of its users to the United States of America and keeps it on servers located in that country.

Legal context

Directive 95/46

3 Recitals 2, 10, 56, 57, 60, 62 and 63 in the preamble to Directive 95/46 are worded as follows:

‘(2) ... data-processing systems are designed to serve man; … they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to … the well-being of individuals;

…

(10) … the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[, signed in Rome on 4 November 1950,] and in the general principles of Community law; …, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

…

(56) … cross-border flows of personal data are necessary to the expansion of international trade; … the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; … the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) … on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

…

(60) … in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

…

(62) … the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) … such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; ...’

4 Articles 1, 2, 25, 26, 28 and 31 of Directive 95/46 provide:

‘*Article 1*

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

...

Article 2

Definitions

For the purposes of this Directive:

(a) “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

...

(d) “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

...

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31(2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorise a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorisations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31(2).

Member States shall take the necessary measures to comply with the Commission's decision.

...

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

— investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

— effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

— the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

...

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

...

Article 31

...

2. Where reference is made to this Article, Articles 4 and 7 of [Council] Decision 1999/468/EC [of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (OJ 1999 L 184, p. 23)] shall apply, having regard to the provisions of Article 8 thereof.

...'

Decision 2000/520

5 Decision 2000/520 was adopted by the Commission on the basis of Article 25(6) of Directive 95/46.

6 Recitals 2, 5 and 8 in the preamble to that decision are worded as follows:

'(2) The Commission may find that a third country ensures an adequate level of protection. In that case personal data may be transferred from the Member States without additional guarantees being necessary.

…

(5) The adequate level of protection for the transfer of data from the Community to the United States recognised by this Decision, should be attained if organisations comply with the safe harbour privacy principles for the protection of personal data transferred from a Member State to the United States (hereinafter "the Principles") and the frequently asked questions (hereinafter "the FAQs") providing guidance for the implementation of the Principles issued by the Government of the United States on 21 July 2000. Furthermore the organisations should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce, or that of another statutory body that will effectively ensure compliance with the Principles implemented in accordance with the FAQs.

…

(8) In the interests of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify in this Decision the exceptional circumstances in which the suspension of specific data flows should be justified, notwithstanding the finding of adequate protection.'

7 Articles 1 to 4 of Decision 2000/520 provide:

‘*Article 1*

1. For the purposes of Article 25(2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the “Safe Harbour Privacy Principles” (hereinafter “the Principles”), as set out in Annex I to this Decision, implemented in accordance with the guidance provided by the frequently asked questions (hereinafter “the FAQs”) issued by the US Department of Commerce on 21 July 2000 as set out in Annex II to this Decision are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States, having regard to the following documents issued by the US Department of Commerce:

(a) the safe harbour enforcement overview set out in Annex III;

(b) a memorandum on damages for breaches of privacy and explicit authorisations in US law set out in Annex IV;

(c) a letter from the Federal Trade Commission set out in Annex V;

(d) a letter from the US Department of Transportation set out in Annex VI.

2. In relation to each transfer of data the following conditions shall be met:

(a) the organisation receiving the data has unambiguously and publicly disclosed its commitment to comply with the Principles implemented in accordance with the FAQs; and

(b) the organisation is subject to the statutory powers of a government body in the United States listed in Annex VII to this Decision which is empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in case of non-compliance with the Principles implemented in accordance with the FAQs.

3. The conditions set out in paragraph 2 are considered to be met for each organisation that self-certifies its adherence to the Principles implemented in accordance with the FAQs from the date on which the organisation notifies to the US Department of Commerce (or its designee) the public disclosure of the commitment referred to in paragraph 2(a) and the identity of the government body referred to in paragraph 2(b).

Article 2

This Decision concerns only the adequacy of protection provided in the United States under the Principles implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC and does not affect the application of other provisions of that Directive that pertain to the processing of personal data within the Member States, in particular Article 4 thereof.

Article 3

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Principles implemented in accordance with the FAQs in order to protect individuals with regard to the processing of their personal data in cases where:

(a) the government body in the United States referred to in Annex VII to this Decision or an independent recourse mechanism within the meaning of letter (a) of the Enforcement Principle set out in Annex I to this Decision has determined that the organisation is violating the Principles implemented in accordance with the FAQs; or

(b) there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

The suspension shall cease as soon as compliance with the Principles implemented in accordance with the FAQs is assured and the competent authorities concerned in the Community are notified thereof.

2. Member States shall inform the Commission without delay when measures are adopted on the basis of paragraph 1.

3. The Member States and the Commission shall also inform each other of cases where the action of bodies responsible for ensuring compliance with the Principles implemented in accordance with the FAQs in the United States fails to secure such compliance.

4. If the information collected under paragraphs 1, 2 and 3 provides evidence that any body responsible for ensuring compliance with the Principles implemented in accordance with the FAQs in the United States is not effectively fulfilling its role, the Commission shall inform the US Department of Commerce and, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC with a view to reversing or suspending the present Decision or limiting its scope.

Article 4

1. This Decision may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the Principles and the FAQs is overtaken by the requirements of US legislation.

The Commission shall in any case evaluate the implementation of the present Decision on the basis of available information three years after its notification to the Member States and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC, including any evidence that could affect the evaluation that the provisions set out in Article 1 of this Decision provide adequate protection within the meaning of Article 25 of Directive 95/46/EC and any evidence that the present Decision is being implemented in a discriminatory way.

2. The Commission shall, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC.'

8 Annex I to Decision 2000/520 is worded as follows:

‘Safe Harbour Privacy Principles issued by the US Department of Commerce on 21 July 2000 ... the Department of Commerce is issuing this document and Frequently Asked Questions (“the Principles”) under its statutory authority to foster, promote, and develop international commerce. The Principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by US organisations receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of “adequacy” it creates. Because the Principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. … Decisions by organisations to qualify for the safe harbour are entirely voluntary, and organisations may qualify for the safe harbour in different ways. ... Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation; or (c) if the effect of the Directive [or] Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organisations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or US law, organisations are expected to opt for the higher protection where possible. ...’

9 Annex II to Decision 2000/520 reads as follows:

‘Frequently Asked Questions (FAQs)

... FAQ 6 — Self-Certification

Q: *How does an organisation self-certify that it adheres to the Safe Harbour Principles?*

A: Safe harbour benefits are assured from the date on which an organisation self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth below.

To self-certify for the safe harbour, organisations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organisation that is joining the safe harbour, that contains at least the following information:

1. name of organisation, mailing address, e-mail address, telephone and fax numbers;

2. description of the activities of the organisation with respect to personal information received from the [European Union]; and

3. description of the organisation’s privacy policy for such personal information, including: (a) where the privacy policy is available for viewing by the public, (b) its effective date of implementation, (c) a contact office for the handling of complaints, access requests, and any other issues arising under the safe harbour, (d) the specific statutory body that has jurisdiction to hear any claims against the organisation regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the

annex to the Principles), (e) name of any privacy programmes in which the organisation is a member, (f) method of verification (e.g. in-house, third party) …, and (g) the independent recourse mechanism that is available to investigate unresolved complaints.

Where the organisation wishes its safe harbour benefits to cover human resources information transferred from the [European Union] for use in the context of the employment relationship, it may do so where there is a statutory body with jurisdiction to hear claims against the organisation arising out of human resources information that is listed in the annex to the Principles. ...

The Department (or its designee) will maintain a list of all organisations that file such letters, thereby assuring the availability of safe harbour benefits, and will update such list on the basis of annual letters and notifications received pursuant to FAQ 11. ...

... FAQ 11 — Dispute Resolution and Enforcement

Q: *How should the dispute resolution requirements of the Enforcement Principle be implemented, and how will an organisation's persistent failure to comply with the Principles be handled?*

A: The Enforcement Principle sets out the requirements for safe harbour enforcement. How to meet the requirements of point (b) of the Principle is set out in the FAQ on verification (FAQ 7). This FAQ 11 addresses points (a) and (c), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Enforcement Principle's requirements. Organisations may satisfy the requirements through the following: (1) compliance with private sector developed privacy programmes that incorporate the Safe Harbour Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle; (2) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (3) commitment to cooperate with data protection authorities located in the European Union or their authorised representatives. This list is intended to be illustrative and not limiting. The private sector may design other mechanisms to provide enforcement, so long as they meet the requirements of the Enforcement Principle and the FAQs. Please note that the Enforcement Principle's requirements are additional to the requirements set forth in paragraph 3 of the introduction to the Principles that self-regulatory efforts must be enforceable under Article 5 of the Federal Trade Commission Act or similar statute.

Recourse Mechanisms

Consumers should be encouraged to raise any complaints they may have with the relevant organisation before proceeding to independent recourse mechanisms. ...

...

FTC Action

The FTC has committed to reviewing on a priority basis referrals received from privacy self-regulatory organisations, such as BBBOnline and TRUSTe, and EU Member States alleging non-compliance with the Safe Harbour Principles to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. ... …'

10 Annex IV to Decision 2000/520 states:

'Damages for Breaches of Privacy, Legal Authorisations and Mergers and Takeovers in US Law

This responds to the request by the European Commission for clarification of US law with respect to (a) claims for damages for breaches of privacy, (b) "explicit authorisations" in US law for the use of personal information in a manner inconsistent with the safe harbour principles, and (c) the effect of mergers and takeovers on obligations undertaken pursuant to the safe harbour principles.

...

B. Explicit Legal Authorisations The safe harbour principles contain an exception where statute, regulation or case-law create "conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the principles is limited to the extent necessary to meet the overriding legitimate interests further[ed] by such authorisation". Clearly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law. As for explicit authorisations, while the safe harbour principles are intended to bridge the differences between the US and European regimes for privacy protection, we owe deference to the legislative prerogatives of our elected lawmakers. The limited exception from strict adherence to the safe harbour principles seeks to strike a balance to accommodate the legitimate interests on each side. The exception is limited to cases where there is an explicit authorisation. Therefore, as a threshold matter, the relevant statute, regulation or court decision must affirmatively authorise the particular conduct by safe harbour organisations ... In other words, the exception would not apply where the law is silent. In addition, the exception would apply only if the explicit authorisation conflicts with adherence to the safe harbour principles. Even then, the exception "is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation". By way of illustration, where the law simply authorises a company to provide personal information to government authorities, the exception would not apply. Conversely, where the law specifically authorises the company to provide personal information to government agencies without the individual's consent, this would constitute an "explicit authorisation" to act in a manner that conflicts with the safe harbour principles. Alternatively, specific exceptions from affirmative requirements to provide notice and consent would fall within the exception (since it would be the equivalent of a specific authorisation to disclose the information without notice and consent). For example, a statute which authorises doctors to provide their patients' medical records to health officials without the patients' prior consent might permit an exception from the notice and choice principles. This authorisation would not permit a doctor to provide the same medical records to health maintenance organisations or commercial pharmaceutical research laboratories, which would be beyond the scope of the purposes authorised by the law and therefore beyond the scope of the exception ... The legal authority in question can be a "stand alone" authorisation to do specific things with personal information, but, as the examples below illustrate, it is likely to be an exception to a broader law which proscribes the collection, use, or disclosure of personal information. ...'

Communication COM(2013) 846 final

11 On 27 November 2013 the Commission adopted the communication to the European Parliament and the Council entitled 'Rebuilding Trust in EU-US Data Flows' (COM(2013) 846 final) ('Communication COM(2013) 846 final'). The communication was accompanied by the 'Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection', also dated 27 November 2013. That report was drawn up, as stated in point 1 thereof, in cooperation with the United States after the existence in that country of a number of surveillance programmes involving the large-scale collection and processing of personal data had been revealed. The report contained inter alia a detailed analysis of United States law as regards, in particular, the legal bases authorising the existence of surveillance programmes and the collection and processing of personal data by United States authorities.

12 In point 1 of Communication COM(2013) 846 final, the Commission stated that '[c]ommercial exchanges are addressed by Decision [2000/520]', adding that '[t]his Decision provides a legal basis for transfers of personal data from the [European Union] to companies established in the [United States] which have adhered to the Safe Harbour Privacy Principles'. In addition, the Commission underlined in point 1 the increasing relevance of personal data flows, owing in particular to the development of the digital economy which has indeed 'led to exponential growth in the quantity, quality, diversity and nature of data processing activities'.

13 In point 2 of that communication, the Commission observed that 'concerns about the level of protection of personal data of [Union] citizens transferred to the [United States] under the Safe Harbour scheme have grown' and that '[t]he voluntary and declaratory nature of the scheme has sharpened focus on its transparency and enforcement'.

14 It further stated in point 2 that '[t]he personal data of [Union] citizens sent to the [United States] under the Safe Harbour may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the [European Union] and the purposes for which it was transferred to the [United States]' and that '[a] majority of the US internet companies that appear to be more directly concerned by [the surveillance] programmes are certified under the Safe Harbour scheme'.

15 In point 3.2 of Communication COM(2013) 846 final, the Commission noted a number of weaknesses in the application of Decision 2000/520. It stated, first, that some certified United States companies did not comply with the principles referred to in Article 1(1) of Decision 2000/520 ('the safe harbour principles') and that improvements had to be made to that decision regarding 'structural shortcomings related to transparency and enforcement, the substantive Safe Harbour principles and the operation of the national security exception'. It observed, secondly, that 'Safe Harbour also acts as a conduit for the transfer of the personal data of EU citizens from the [European Union] to the [United States] by companies required to surrender data to US intelligence agencies under the US intelligence collection programmes'.

16 The Commission concluded in point 3.2 that whilst, '[g]iven the weaknesses identified, the current implementation of Safe Harbour cannot be maintained, ... its revocation would[, however,] adversely affect the interests of member companies in the [European Union] and in the [United States]'. Finally, the Commission added in that point that it would 'engage with the US authorities to discuss the shortcomings identified'.

Communication COM(2013) 847 final

17 On the same date, 27 November 2013, the Commission adopted the communication to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the [European Union] (COM(2013) 847 final) ('Communication COM(2013) 847 final'). As is clear from point 1 thereof, that communication was based inter alia on information received in the ad hoc EU-US Working Group and followed two Commission assessment reports published in 2002 and 2004 respectively.

18 Point 1 of Communication COM(2013) 847 final explains that the functioning of Decision 2000/520 'relies on commitments and self-certification of adhering companies', adding that '[s]igning up to these arrangements is voluntary, but the rules are binding for those who sign up'.

19 In addition, it is apparent from point 2.2 of Communication COM(2013) 847 final that, as at 26 September 2013, 3 246 companies, falling within many industry and services sectors, were certified. Those companies mainly provided services in the EU internal market, in particular in the internet

sector, and some of them were EU companies which had subsidiaries in the United States. Some of those companies processed the data of their employees in Europe which was transferred to the United States for human resource purposes.

20 The Commission stated in point 2.2 that '[a]ny gap in transparency or in enforcement on the US side results in responsibility being shifted to European data protection authorities and to the companies which use the scheme'.

21 It is apparent, in particular, from points 3 to 5 and 8 of Communication COM(2013) 847 final that, in practice, a significant number of certified companies did not comply, or did not comply fully, with the safe harbour principles.

22 In addition, the Commission stated in point 7 of Communication COM(2013) 847 final that 'all companies involved in the PRISM programme [a large-scale intelligence collection programme], and which grant access to US authorities to data stored and processed in the [United States], appear to be Safe Harbour certified' and that '[t]his has made the Safe Harbour scheme one of the conduits through which access is given to US intelligence authorities to collecting personal data initially processed in the [European Union]'. In that regard, the Commission noted in point 7.1 of that communication that 'a number of legal bases under US law allow large-scale collection and processing of personal data that is stored or otherwise processed [by] companies based in the [United States]' and that '[t]he large-scale nature of these programmes may result in data transferred under Safe Harbour being accessed and further processed by US authorities beyond what is strictly necessary and proportionate to the protection of national security as foreseen under the exception provided in [Decision 2000/520]'.

23 In point 7.2 of Communication COM(2013) 847 final, headed 'Limitations and redress possibilities', the Commission noted that 'safeguards that are provided under US law are mostly available to US citizens or legal residents' and that, '[m]oreover, there are no opportunities for either EU or US data subjects to obtain access, rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the US surveillance programmes'.

24 According to point 8 of Communication COM(2013) 847 final, the certified companies included '[w]eb companies such as Google, Facebook, Microsoft, Apple, Yahoo', which had 'hundreds of millions of clients in Europe' and transferred personal data to the United States for processing.

25 The Commission concluded in point 8 that 'the large-scale access by intelligence agencies to data transferred to the [United States] by Safe Harbour certified companies raises additional serious questions regarding the continuity of data protection rights of Europeans when their data is transferred to the [United States]'.

The dispute in the main proceedings and the questions referred for a preliminary ruling

26 Mr Schrems, an Austrian national residing in Austria, has been a user of the Facebook social network ('Facebook') since 2008.

27 Any person residing in the European Union who wishes to use Facebook is required to conclude, at the time of his registration, a contract with Facebook Ireland, a subsidiary of Facebook Inc. which is itself established in the United States. Some or all of the personal data of Facebook Ireland's users who reside in the European Union is transferred to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing.

28 On 25 June 2013 Mr Schrems made a complaint to the Commissioner by which he in essence asked the latter to exercise his statutory powers by prohibiting Facebook Ireland from transferring his personal data to the United States. He contended in his complaint that the law and practice in force in that country did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities. Mr Schrems referred in this regard to the revelations made by Edward Snowden concerning the activities of the United States intelligence services, in particular those of the National Security Agency ('the NSA').

29 Since the Commissioner took the view that he was not required to investigate the matters raised by Mr Schrems in the complaint, he rejected it as unfounded. The Commissioner considered that there was no evidence that Mr Schrems' personal data had been accessed by the NSA. He added that the allegations raised by Mr Schrems in his complaint could not be profitably put forward since any question of the adequacy of data protection in the United States had to be determined in accordance with Decision 2000/520 and the Commission had found in that decision that the United States ensured an adequate level of protection.

30 Mr Schrems brought an action before the High Court challenging the decision at issue in the main proceedings. After considering the evidence adduced by the parties to the main proceedings, the High Court found that the electronic surveillance and interception of personal data transferred from the European Union to the United States serve necessary and indispensable objectives in the public interest. However, it added that the revelations made by Edward Snowden had demonstrated a 'significant over-reach' on the part of the NSA and other federal agencies.

31 According to the High Court, Union citizens have no effective right to be heard. Oversight of the intelligence services' actions is carried out within the framework of an *ex parte* and secret procedure. Once the personal data has been transferred to the United States, it is capable of being accessed by the NSA and other federal agencies, such as the Federal Bureau of Investigation (FBI), in the course of the indiscriminate surveillance and interception carried out by them on a large scale.

32 The High Court stated that Irish law precludes the transfer of personal data outside national territory save where the third country ensures an adequate level of protection for privacy and fundamental rights and freedoms. The importance of the rights to privacy and to inviolability of the dwelling, which are guaranteed by the Irish Constitution, requires that any interference with those rights be proportionate and in accordance with the law.

33 The High Court held that the mass and undifferentiated accessing of personal data is clearly contrary to the principle of proportionality and the fundamental values protected by the Irish Constitution. In order for interception of electronic communications to be regarded as consistent with the Irish Constitution, it would be necessary to demonstrate that the interception is targeted, that the surveillance of certain persons or groups of persons is objectively justified in the interests of national security or the suppression of crime and that there are appropriate and verifiable safeguards. Thus, according to the High Court, if the main proceedings were to be disposed of on the basis of Irish law alone, it would then have to be found that, given the existence of a serious doubt as to whether the United States ensures an adequate level of protection of personal data, the Commissioner should have proceeded to investigate the matters raised by Mr Schrems in his complaint and that the Commissioner was wrong in rejecting the complaint.

34 However, the High Court considers that this case concerns the implementation of EU law as referred to in Article 51 of the Charter and that the legality of the decision at issue in the main proceedings must therefore be assessed in the light of EU law. According to the High Court, Decision 2000/520 does not satisfy the requirements flowing both from Articles 7 and 8 of the Charter and from the principles set out by the Court of Justice in the judgment in *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238). The right to respect for private life, guaranteed by Article 7 of the Charter and by the core values common to the traditions of the Member States, would be

rendered meaningless if the State authorities were authorised to access electronic communications on a casual and generalised basis without any objective justification based on considerations of national security or the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards.

35 The High Court further observes that in his action Mr Schrems in reality raises the legality of the safe harbour regime which was established by Decision 2000/520 and gives rise to the decision at issue in the main proceedings. Thus, even though Mr Schrems has not formally contested the validity of either Directive 95/46 or Decision 2000/520, the question is raised, according to the High Court, as to whether, on account of Article 25(6) of Directive 95/46, the Commissioner was bound by the Commission's finding in Decision 2000/520 that the United States ensures an adequate level of protection or whether Article 8 of the Charter authorised the Commissioner to break free, if appropriate, from such a finding.

36 In those circumstances the High Court decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'(1) Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding?

(2) Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published?'

Consideration of the questions referred

37 By its questions, which it is appropriate to examine together, the referring court asks, in essence, whether and to what extent Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, prevents a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from being able to examine the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

The powers of the national supervisory authorities, within the meaning of Article 28 of Directive 95/46, when the Commission has adopted a decision pursuant to Article 25(6) of that directive

38 It should be recalled first of all that the provisions of Directive 95/46, inasmuch as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to respect for private life, must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter (see judgments in *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 68; *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraph 68; and *Ryneš*, C-212/13, EU:C:2014:2428, paragraph 29).

39 It is apparent from Article 1 of Directive 95/46 and recitals 2 and 10 in its preamble that that directive seeks to ensure not only effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the fundamental right to respect for private life with regard to the processing of personal data, but also a high level of protection of those fundamental rights and freedoms. The importance of both the fundamental right to respect for private life, guaranteed by Article 7 of the Charter, and the fundamental right to the protection of personal data, guaranteed by Article 8 thereof, is, moreover, emphasised in the case-law of the Court (see judgments in *Rijkeboer*, C-553/07, EU:C:2009:293, paragraph 47; *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 53; and *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraphs, 53, 66, 74 and the case-law cited).

40 As regards the powers available to the national supervisory authorities in respect of transfers of personal data to third countries, it should be noted that Article 28(1) of Directive 95/46 requires Member States to set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of such data. In addition, that requirement derives from the primary law of the European Union, in particular Article 8(3) of the Charter and Article 16(2) TFEU (see, to this effect, judgments in *Commission* v *Austria*, C-614/10, EU:C:2012:631, paragraph 36, and *Commission* v *Hungary*, C-288/12, EU:C:2014:237, paragraph 47).

41 The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established in order to strengthen the protection of individuals and bodies affected by the decisions of those authorities. The establishment in Member States of independent supervisory authorities is therefore, as stated in recital 62 in the preamble to Directive 95/46, an essential component of the protection of individuals with regard to the processing of personal data (see judgments in *Commission* v *Germany*, C-518/07, EU:C:2010:125, paragraph 25, and *Commission* v *Hungary*, C-288/12, EU:C:2014:237, paragraph 48 and the case-law cited).

42 In order to guarantee that protection, the national supervisory authorities must, in particular, ensure a fair balance between, on the one hand, observance of the fundamental right to privacy and, on the other hand, the interests requiring free movement of personal data (see, to this effect, judgments in *Commission* v *Germany*, C-518/07, EU:C:2010:125, paragraph 24, and *Commission* v *Hungary*, C-288/12, EU:C:2014:237, paragraph 51).

43 The national supervisory authorities have a wide range of powers for that purpose. Those powers, listed on a non-exhaustive basis in Article 28(3) of Directive 95/46, constitute necessary means to perform their duties, as stated in recital 63 in the preamble to the directive. Thus, those authorities possess, in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings.

44 It is, admittedly, apparent from Article 28(1) and (6) of Directive 95/46 that the powers of the national supervisory authorities concern processing of personal data carried out on the territory of their own Member State, so that they do not have powers on the basis of Article 28 in respect of processing of such data carried out in a third country.

45 However, the operation consisting in having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 2(b) of Directive 95/46 (see, to this effect, judgment in *Parliament* v *Council and Commission*, C-317/04 and C-318/04, EU:C:2006:346, paragraph 56) carried out in a Member State. That provision defines ‘processing of

personal data' as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means' and mentions, by way of example, 'disclosure by transmission, dissemination or otherwise making available'.

46 Recital 60 in the preamble to Directive 95/46 states that transfers of personal data to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to the directive. In that regard, Chapter IV of the directive, in which Articles 25 and 26 appear, has set up a regime intended to ensure that the Member States oversee transfers of personal data to third countries. That regime is complementary to the general regime set up by Chapter II of the directive laying down the general rules on the lawfulness of the processing of personal data (see, to this effect, judgment in *Lindqvist*, C-101/01, EU:C:2003:596, paragraph 63).

47 As, in accordance with Article 8(3) of the Charter and Article 28 of Directive 95/46, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of individuals with regard to the processing of personal data, each of them is therefore vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down by Directive 95/46.

48 Whilst acknowledging, in recital 56 in its preamble, that transfers of personal data from the Member States to third countries are necessary for the expansion of international trade, Directive 95/46 lays down as a principle, in Article 25(1), that such transfers may take place only if the third country ensures an adequate level of protection.

49 Furthermore, recital 57 states that transfers of personal data to third countries not ensuring an adequate level of protection must be prohibited.

50 In order to control transfers of personal data to third countries according to the level of protection accorded to it in each of those countries, Article 25 of Directive 95/46 imposes a series of obligations on the Member States and the Commission. It is apparent, in particular, from that article that the finding that a third country does or does not ensure an adequate level of protection may, as the Advocate General has observed in point 86 of his Opinion, be made either by the Member States or by the Commission.

51 The Commission may adopt, on the basis of Article 25(6) of Directive 95/46, a decision finding that a third country ensures an adequate level of protection. In accordance with the second subparagraph of that provision, such a decision is addressed to the Member States, who must take the measures necessary to comply with it. Pursuant to the fourth paragraph of Article 288 TFEU, it is binding on all the Member States to which it is addressed and is therefore binding on all their organs (see, to this effect, judgments in *Albako Margarinefabrik*, 249/85, EU:C:1987:245, paragraph 17, and *Mediaset*, C-69/13, EU:C:2014:71, paragraph 23) in so far as it has the effect of authorising transfers of personal data from the Member States to the third country covered by it.

52 Thus, until such time as the Commission decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, admittedly cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection. Measures of the EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality (judgment in *Commission* v *Greece*, C-475/01, EU:C:2004:585, paragraph 18 and the case-law cited).

53 However, a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, such as Decision 2000/520, cannot prevent persons whose personal data has been or could be transferred to a third country from lodging with the national supervisory authorities a claim, within the meaning of

Article 28(4) of that directive, concerning the protection of their rights and freedoms in regard to the processing of that data. Likewise, as the Advocate General has observed in particular in points 61, 93 and 116 of his Opinion, a decision of that nature cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 28 of the directive.

54 Neither Article 8(3) of the Charter nor Article 28 of Directive 95/46 excludes from the national supervisory authorities' sphere of competence the oversight of transfers of personal data to third countries which have been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46.

55 In particular, the first subparagraph of Article 28(4) of Directive 95/46, under which the national supervisory authorities are to hear 'claims lodged by any person … concerning the protection of his rights and freedoms in regard to the processing of personal data', does not provide for any exception in this regard where the Commission has adopted a decision pursuant to Article 25(6) of that directive.

56 Furthermore, it would be contrary to the system set up by Directive 95/46 and to the objective of Articles 25 and 28 thereof for a Commission decision adopted pursuant to Article 25(6) to have the effect of preventing a national supervisory authority from examining a person's claim concerning the protection of his rights and freedoms in regard to the processing of his personal data which has been or could be transferred from a Member State to the third country covered by that decision.

57 On the contrary, Article 28 of Directive 95/46 applies, by its very nature, to any processing of personal data. Thus, even if the Commission has adopted a decision pursuant to Article 25(6) of that directive, the national supervisory authorities, when hearing a claim lodged by a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the directive.

58 If that were not so, persons whose personal data has been or could be transferred to the third country concerned would be denied the right, guaranteed by Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim for the purpose of protecting their fundamental rights (see, by analogy, judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 68).

59 A claim, within the meaning of Article 28(4) of Directive 95/46, by which a person whose personal data has been or could be transferred to a third country contends, as in the main proceedings, that, notwithstanding what the Commission has found in a decision adopted pursuant to Article 25(6) of that directive, the law and practices of that country do not ensure an adequate level of protection must be understood as concerning, in essence, whether that decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals.

60 In this connection, the Court's settled case-law should be recalled according to which the European Union is a union based on the rule of law in which all acts of its institutions are subject to review of their compatibility with, in particular, the Treaties, general principles of law and fundamental rights (see, to this effect, judgments in *Commission and Others* v *Kadi*, C-584/10 P, C-593/10 P and C-595/10 P, EU:C:2013:518, paragraph 66; *Inuit Tapiriit Kanatami and Others* v *Parliament and Council*, C-583/11 P, EU:C:2013:625, paragraph 91; and *Telefónica* v *Commission*, C-274/12 P, EU:C:2013:852, paragraph 56). Commission decisions adopted pursuant to Article 25(6) of Directive 95/46 cannot therefore escape such review.

61 That said, the Court alone has jurisdiction to declare that an EU act, such as a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, is invalid, the exclusivity of that jurisdiction having the purpose of guaranteeing legal certainty by ensuring that EU law is applied uniformly (see judgments in *Melki and Abdeli*, C-188/10 and C-189/10, EU:C:2010:363, paragraph 54, and *CIVAD*, C-533/10, EU:C:2012:347, paragraph 40).

62 Whilst the national courts are admittedly entitled to consider the validity of an EU act, such as a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, they are not, however, endowed with the power to declare such an act invalid themselves (see, to this effect, judgments in *Foto-Frost*, 314/85, EU:C:1987:452, paragraphs 15 to 20, and *IATA and ELFAA*, C-344/04, EU:C:2006:10, paragraph 27). A fortiori, when the national supervisory authorities examine a claim, within the meaning of Article 28(4) of that directive, concerning the compatibility of a Commission decision adopted pursuant to Article 25(6) of the directive with the protection of the privacy and of the fundamental rights and freedoms of individuals, they are not entitled to declare that decision invalid themselves.

63 Having regard to those considerations, where a person whose personal data has been or could be transferred to a third country which has been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46 lodges with a national supervisory authority a claim concerning the protection of his rights and freedoms in regard to the processing of that data and contests, in bringing the claim, as in the main proceedings, the compatibility of that decision with the protection of the privacy and of the fundamental rights and freedoms of individuals, it is incumbent upon the national supervisory authority to examine the claim with all due diligence.

64 In a situation where the national supervisory authority comes to the conclusion that the arguments put forward in support of such a claim are unfounded and therefore rejects it, the person who lodged the claim must, as is apparent from the second subparagraph of Article 28(3) of Directive 95/46, read in the light of Article 47 of the Charter, have access to judicial remedies enabling him to challenge such a decision adversely affecting him before the national courts. Having regard to the case-law cited in paragraphs 61 and 62 of the present judgment, those courts must stay proceedings and make a reference to the Court for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case may be, raised by them of their own motion are well founded (see, to this effect, judgment in *T & L Sugars and Sidul Açúcares* v *Commission*, C-456/13 P, EU:C:2015:284, paragraph 48 and the case-law cited).

65 In the converse situation, where the national supervisory authority considers that the objections advanced by the person who has lodged with it a claim concerning the protection of his rights and freedoms in regard to the processing of his personal data are well founded, that authority must, in accordance with the third indent of the first subparagraph of Article 28(3) of Directive 95/46, read in the light in particular of Article 8(3) of the Charter, be able to engage in legal proceedings. It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity.

66 Having regard to the foregoing considerations, the answer to the questions referred is that Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the

processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

The validity of Decision 2000/520

67 As is apparent from the referring court's explanations relating to the questions submitted, Mr Schrems contends in the main proceedings that United States law and practice do not ensure an adequate level of protection within the meaning of Article 25 of Directive 95/46. As the Advocate General has observed in points 123 and 124 of his Opinion, Mr Schrems expresses doubts, which the referring court indeed seems essentially to share, concerning the validity of Decision 2000/520. In such circumstances, having regard to what has been held in paragraphs 60 to 63 of the present judgment and in order to give the referring court a full answer, it should be examined whether that decision complies with the requirements stemming from Directive 95/46 read in the light of the Charter.

The requirements stemming from Article 25(6) of Directive 95/46

68 As has already been pointed out in paragraphs 48 and 49 of the present judgment, Article 25(1) of Directive 95/46 prohibits transfers of personal data to a third country not ensuring an adequate level of protection.

69 However, for the purpose of overseeing such transfers, the first subparagraph of Article 25(6) of Directive 95/46 provides that the Commission 'may find … that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into …, for the protection of the private lives and basic freedoms and rights of individuals'.

70 It is true that neither Article 25(2) of Directive 95/46 nor any other provision of the directive contains a definition of the concept of an adequate level of protection. In particular, Article 25(2) does no more than state that the adequacy of the level of protection afforded by a third country 'shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations' and lists, on a non-exhaustive basis, the circumstances to which consideration must be given when carrying out such an assessment.

71 However, first, as is apparent from the very wording of Article 25(6) of Directive 95/46, that provision requires that a third country 'ensures' an adequate level of protection by reason of its domestic law or its international commitments. Secondly, according to the same provision, the adequacy of the protection ensured by the third country is assessed 'for the protection of the private lives and basic freedoms and rights of individuals'.

72 Thus, Article 25(6) of Directive 95/46 implements the express obligation laid down in Article 8(1) of the Charter to protect personal data and, as the Advocate General has observed in point 139 of his Opinion, is intended to ensure that the high level of that protection continues where personal data is transferred to a third country.

73 The word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph of the present judgment would be disregarded. Furthermore, the

high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries.

74 It is clear from the express wording of Article 25(6) of Directive 95/46 that it is the legal order of the third country covered by the Commission decision that must ensure an adequate level of protection. Even though the means to which that third country has recourse, in this connection, for the purpose of ensuring such a level of protection may differ from those employed within the European Union in order to ensure that the requirements stemming from Directive 95/46 read in the light of the Charter are complied with, those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union.

75 Accordingly, when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the applicable rules in that country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules, since it must, under Article 25(2) of Directive 95/46, take account of all the circumstances surrounding a transfer of personal data to a third country.

76 Also, in the light of the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted a decision pursuant to Article 25(6) of Directive 95/46, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard.

77 Moreover, as the Advocate General has stated in points 134 and 135 of his Opinion, when the validity of a Commission decision adopted pursuant to Article 25(6) of Directive 95/46 is examined, account must also be taken of the circumstances that have arisen after that decision's adoption.

78 In this regard, it must be stated that, in view of, first, the important role played by the protection of personal data in the light of the fundamental right to respect for private life and, secondly, the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country not ensuring an adequate level of protection, the Commission's discretion as to the adequacy of the level of protection ensured by a third country is reduced, with the result that review of the requirements stemming from Article 25 of Directive 95/46, read in the light of the Charter, should be strict (see, by analogy, judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 47 and 48).

Article 1 of Decision 2000/520

79 The Commission found in Article 1(1) of Decision 2000/520 that the principles set out in Annex I thereto, implemented in accordance with the guidance provided by the FAQs set out in Annex II, ensure an adequate level of protection for personal data transferred from the European Union to organisations established in the United States. It is apparent from that provision that both those principles and the FAQs were issued by the United States Department of Commerce.

80 An organisation adheres to the safe harbour principles on the basis of a system of self-certification, as is apparent from Article 1(2) and (3) of Decision 2000/520, read in conjunction with FAQ 6 set out in Annex II thereto.

81 Whilst recourse by a third country to a system of self-certification is not in itself contrary to the requirement laid down in Article 25(6) of Directive 95/46 that the third country concerned must ensure an adequate level of protection 'by reason of its domestic law or … international commitments', the reliability of such a system, in the light of that requirement, is founded essentially

on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be identified and punished in practice.

82 In the present instance, by virtue of the second paragraph of Annex I to Decision 2000/520, the safe harbour principles are 'intended for use solely by US organisations receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of "adequacy" it creates'. Those principles are therefore applicable solely to self-certified United States organisations receiving personal data from the European Union, and United States public authorities are not required to comply with them.

83 Moreover, Decision 2000/520, pursuant to Article 2 thereof, 'concerns only the adequacy of protection provided in the United States under the [safe harbour principles] implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive [95/46]', without, however, containing sufficient findings regarding the measures by which the United States ensures an adequate level of protection, within the meaning of Article 25(6) of that directive, by reason of its domestic law or its international commitments.

84 In addition, under the fourth paragraph of Annex I to Decision 2000/520, the applicability of the safe harbour principles may be limited, in particular, 'to the extent necessary to meet national security, public interest, or law enforcement requirements' and 'by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation'.

85 In this connection, Decision 2000/520 states in Part B of Annex IV, with regard to the limits to which the safe harbour principles' applicability is subject, that, '[c]learly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law'.

86 Thus, Decision 2000/520 lays down that 'national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them.

87 In the light of the general nature of the derogation set out in the fourth paragraph of Annex I to Decision 2000/520, that decision thus enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States. To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference (judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 33 and the case-law cited).

88 In addition, Decision 2000/520 does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security.

89 Nor does Decision 2000/520 refer to the existence of effective legal protection against interference of that kind. As the Advocate General has observed in points 204 to 206 of his Opinion, procedures before the Federal Trade Commission — the powers of which, described in particular in FAQ 11 set

out in Annex II to that decision, are limited to commercial disputes — and the private dispute resolution mechanisms concern compliance by the United States undertakings with the safe harbour principles and cannot be applied in disputes relating to the legality of interference with fundamental rights that results from measures originating from the State.

90 Moreover, the foregoing analysis of Decision 2000/520 is borne out by the Commission's own assessment of the situation resulting from the implementation of that decision. Particularly in points 2 and 3.2 of Communication COM(2013) 846 final and in points 7.1, 7.2 and 8 of Communication COM(2013) 847 final, the content of which is set out in paragraphs 13 to 16 and paragraphs 22, 23 and 25 of the present judgment respectively, the Commission found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.

91 As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data (judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 54 and 55 and the case-law cited).

92 Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary (judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 52 and the case-law cited).

93 Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail (see, to this effect, concerning Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 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 2006 L 105, p. 54), judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 57 to 61).

94 In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (see, to this effect, judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 39).

95 Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an

effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law (see, to this effect, judgments in *Les Verts* v *Parliament*, 294/83, EU:C:1986:166, paragraph 23; *Johnston*, 222/84, EU:C:1986:206, paragraphs 18 and 19; *Heylens and Others*, 222/86, EU:C:1987:442, paragraph 14; and *UGT-Rioja and Others*, C-428/06 to C-434/06, EU:C:2008:488, paragraph 80).

96 As has been found in particular in paragraphs 71, 73 and 74 of the present judgment, in order for the Commission to adopt a decision pursuant to Article 25(6) of Directive 95/46, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order, a level that is apparent in particular from the preceding paragraphs of the present judgment.

97 However, the Commission did not state, in Decision 2000/520, that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments.

98 Consequently, without there being any need to examine the content of the safe harbour principles, it is to be concluded that Article 1 of Decision 2000/520 fails to comply with the requirements laid down in Article 25(6) of Directive 95/46, read in the light of the Charter, and that it is accordingly invalid.

Article 3 of Decision 2000/520

99 It is apparent from the considerations set out in paragraphs 53, 57 and 63 of the present judgment that, under Article 28 of Directive 95/46, read in the light in particular of Article 8 of the Charter, the national supervisory authorities must be able to examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to him. That is in particular the case where, in bringing such a claim, that person raises questions regarding the compatibility of a Commission decision adopted pursuant to Article 25(6) of that directive with the protection of the privacy and of the fundamental rights and freedoms of individuals.

100 However, the first subparagraph of Article 3(1) of Decision 2000/520 lays down specific rules regarding the powers available to the national supervisory authorities in the light of a Commission finding relating to an adequate level of protection, within the meaning of Article 25 of Directive 95/46.

101 Under that provision, the national supervisory authorities may, '[w]ithout prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive [95/46], … suspend data flows to an organisation that has self-certified its adherence to the [principles of Decision 2000/520]', under restrictive conditions establishing a high threshold for intervention. Whilst that provision is without prejudice to the powers of those authorities to take action to ensure compliance with national provisions adopted pursuant to Directive 95/46, it excludes, on the other hand, the possibility of them taking action to ensure compliance with Article 25 of that directive.

102 The first subparagraph of Article 3(1) of Decision 2000/520 must therefore be understood as denying the national supervisory authorities the powers which they derive from Article 28 of Directive 95/46, where a person, in bringing a claim under that provision, puts forward matters that may call into question whether a Commission decision that has found, on the basis of Article 25(6) of the directive, that a third country ensures an adequate level of protection is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals.

103 The implementing power granted by the EU legislature to the Commission in Article 25(6) of Directive 95/46 does not confer upon it competence to restrict the national supervisory authorities' powers referred to in the previous paragraph of the present judgment.

104 That being so, it must be held that, in adopting Article 3 of Decision 2000/520, the Commission exceeded the power which is conferred upon it in Article 25(6) of Directive 95/46, read in the light of the Charter, and that Article 3 of the decision is therefore invalid.

105 As Articles 1 and 3 of Decision 2000/520 are inseparable from Articles 2 and 4 of that decision and the annexes thereto, their invalidity affects the validity of the decision in its entirety.

106 Having regard to all the foregoing considerations, it is to be concluded that Decision 2000/520 is invalid.

Costs

107 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Grand Chamber) hereby rules:

1. **Article 25(6) of 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 as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003, read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.**

2. **Decision 2000/520 is invalid.**

[Signatures]

Appendix 2:

Data transfers between the EU and UK post Brexit?
Andrew D. Murray
International Data Privacy Law, 2017, Vol. 7, No. 3

Data transfers between the EU and UK post Brexit?

Andrew D. Murray*

Key Points

- Changes to the UK constitutional and institutional settlement on Brexit day may affect the likelihood of the UK securing an adequacy decision under GDPR.
- Despite the UK Government claiming that on Brexit day, 'it will have fully implemented EU [data] privacy rules' it will have no equivalent of Article 8 of the EU Charter in domestic law.
- This may undermine efforts to achieve an adequacy ruling due to the decision of the CJEU in *Maximillian Schrems v Data Protection Commissioner*.
- The UK's decision to continue with a data retention regime in Part 4 of the Investigatory Powers Act 2016 could also be at odds with the Article 8, Charter right.
- Conflict between the domestic legal settlement of the Investigatory Powers Act 2016 and the decision of the CJEU in *Tele2 Sverige AB v Post-och telestyrelsen* may also imperil an adequacy decision.

Introduction: the UK government's position

On 1 February 2017, Matt Hancock, Minister of State for Digital and Culture, and part of the UK Government team responsible for policy in relation to data protection, as well as implementation of the General Data Protection Regulation (GDPR), appeared before the EU Home Affairs Sub-Committee. The Committee were keen to hear from the Minister the Government's plans to ensure the continued flow of data from the EU to the UK after Brexit. Confirming that the UK Government intended to implement the GDPR fully, and that they would not seek to make any significant changes to UK data protection law post Brexit, he noted that the Government was 'keen to secure the unhindered flow of data between the UK and the EU post-Brexit and we think that signing up to the GDPR data protection rules is an important part of helping to deliver that'.[1] While the Minister was keen to stress the UK Government would seek to ensure the unhindered exchange of data within an appropriate data protection environment he would not be drawn on whether the UK Government believed an adequacy decision would be necessary before 'Brexit Day' on 29 March 2019 (assuming no extensions to negotiations) and refused to be drawn on the processes while negotiations were ongoing. When directly asked the question 'If you do not secure an adequacy decision what is the default position?' the Minister responded rather blandly 'we are seeking unhindered data flows, and that we are confident we will achieve'.[2]

In a later appearance before the same Sub-Committee, Baroness Williams, Minister of State at the Home Office placed on the record 'the importance that the Government places on Data Protection and [their] commitment to ensuring robust safeguards are in place'.[3] She argued that 'the U.K. will enjoy a unique position as a third country seeking data transfers with the EU, given that, unlike other non-EU countries, it will have fully implemented EU [data] privacy rules'.[4] Like her colleague Mr Hancock though she refused to be drawn on the details of any post-Brexit settlement.

* Department of Law, London School of Economics, London, UK. Email: a.murray@lse.ac.uk. The author would like to thank Dr Orla Lynskey, the anonymous referees, and the editors for comments on earlier drafts. In addition, thanks are due to the participants of the Irish Centre for European Law Privacy and Data Protection Conference 2017.

1 The Rt. Hon Matt Hancock, evidence to the EU Home Affairs Sub-Committee, 1 February 2017 <http://www.parliamentlive.tv/Event/Index/b3334d4c-93bf-4aca-9df5-666b7a72c06c> accessed 1 August 2017, 10:49:32–10:49:53.

2 Ibid 11:02:35–11:03:03.

3 Baroness Williams of Trafford, evidence to the EU Home Affairs Sub-Committee, 26 April 2017 <http://parliamentlive.tv/Event/Index/ed6b1fe1-c786-4768-9e63-a65b994cc8d7> accessed 1 August 2017, 11:02:50–11:03:07

4 Ibid 11:08:17–11:08:24.

It is clear therefore that the position of the UK Government is that the UK will continue to trade data with EU27 states following Brexit and that this should be 'unhindered'. It also appears to be the view of the Government that to achieve a settlement to allow this to happen will be quite uncontentious given that in the words of Baroness Williams, 'obviously on the day that we leave our laws are compatible with those of the EU';[5] however, this article will argue that this is not as clear-cut as Government Ministers seem to be assuming. The morning we leave the EU a number of institutional and constitutional differences will occur. Baroness Janke, in a question to Mr Hancock, alluded to at least one of those differences: 'If we will no longer be under the Jurisdiction of the European Court of Justice, how do you anticipate who will be the [] final adjudicator in such matters?'[6] This is a significant question given in Recital 41 of the GDPR:

> [w]here this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, ***in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights***.[7]

The significance of Recital 41 should not be underestimated for reasons we shall see below. The response from Mr Hancock was in light of this less than encouraging phrase: 'there are several different ways that that can take place but [] we don't have the answer to that question.'[8]

Brexit and the fundamental right to data protection

Brexit will have legal implications far beyond the sphere of data protection and while data protection and data transference may be described as a 'high priority' by Minsters[9] it must compete for attention alongside other 'high priorities' such as immigration controls; a common travel area with Ireland; investment in science and innovation; and a common approach to fighting crime and terrorism. All of these were listed as being among the Government's 12 priorities for Brexit in the Prime Minister's speech of 17 January 2017, which pointedly did not list data protection and data transference among her priorities.[10] This may explain the apparent approach of the Government: to serendipitously continue to apply in domestic law the GDPR and related Directives that will have come into effect on or by 25 May 2018 in full; to ensure in their words 'an uninterrupted and unhindered' flow of data between the UK and EU27 post Brexit. However, as Baroness Janke explored, much of the constitutional and institutional landscape will be very different on 29 March 2019. The EU institutions will be out with the UK's legal and constitutional framework and thus institutions such as the Commission and the Court of Justice will have no direct authority. The UK will also no longer be a member of the new European Data Protection Board (EDPB), for the Board is 'composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives'.[11]

The EDPB is considerably more powerful than the Article 29 Working Party with expanded roles and influence. The EDPB shall be an EU body[12] and will have specific legal authority to act independently.[13] The EDPB will be tasked with ensuring consistency of GDPR application throughout the EU and will issue guidelines and opinions to supervisory authorities when certain measures are adopted.[14] A key role of the EDPB will be to issue binding decisions where conflicts arise between supervisory authorities, giving the EDPB a quasi-judicial function.[15] Further, and crucially for the UK, the EDPB under is tasked with 'provid[ing] the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection'.[16] Thus the

5 Ibid 11:10:29–11:10:36.

6 Above n 1, 10:40:30–10:40:58.

7 Emphasis added.

8 Above n 1, 10:40:58–10:41:06.

9 Statement of Matt Hancock to the House of Lords European Union Committee as recorded at para 143 in Brexit: the EU data protection package, 3rd Report of Session 2017–18. <https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/7.pdf> accessed 1 August 2017.

10 The Rt. Hon Theresa May MP, *The Government's Negotiating Objectives for Exiting the EU*, 17 January 2017. <https://www.gov.uk/government/speeches/the-governments-negotiating-objectives-for-exiting-the-eu-pm-speech> accessed 1 August 2017.

11 Regulation (EU) 2016/679 of the European Parliament 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), Art 68(3), OJ 2016 L 119/1.

12 Ibid art 68(1).

13 Ibid art 69(1).

14 Ibid arts 64, 70.

15 Ibid art 65.

16 Ibid art 70(1)(s).

EDPB will advise the Commission of the UK's adequacy under the GDPR but more importantly will continue to monitor the UK's compliance. This suggests that should the UK fail to accept any decision of the EDPB, it may lose its adequacy status. This means the UK will have to accept decisions of the EDPB without representation on the Board, a position likely to be quite unpalatable to those who view Brexit as a complete divorce from EU institutions.

The UK's rights framework will also change for, as the UK Government White Paper on the Great Repeal Bill states:

> The Charter (of Fundamental Rights) only applies to member states when acting within the scope of EU law, so its relevance is removed by our withdrawal from the EU . . . . It cannot be right that the Charter could be used to bring challenges against the Government, or for UK legislation after our withdrawal to be struck down on the basis of the Charter. On that basis ***the Charter will not be converted into UK law by the Great Repeal Bill***.'[17]

The White Paper suggests that withdrawal from the EU Charter will cause no change to the established rights framework of the UK:

> The Government's intention is that the removal of the Charter from UK law ***will not affect the substantive rights that individuals already benefit from in the UK***. Many of these underlying rights exist elsewhere in the body of EU law which we will be converting into UK law. Others already exist in UK law, or in international agreements to which the UK is a party. As EU law is converted into UK law by the Great Repeal Bill, it will continue to be interpreted by UK courts in a way that is consistent with those underlying rights. Insofar as cases have been decided by reference to those underlying rights, that case law will continue to be relevant. In addition, insofar as such cases refer to the Charter, that element will have to be read as referring only to the underlying rights, rather than to the Charter itself.[18]

One specific right, which is not to be found in UK law, or in other international agreements, is Article 8 of the EU Charter:[19] the Data Protection Right. Clearly, the UK Government will point to their intention to implement the GDPR as evidence that data protection rights are included in that body of 'underlying rights [which] exist elsewhere in the body of EU law which we will be converting into UK law'.[20] However it may be argued that there is a difference between the fundamental right to data protection found in the Article 8, and the provisions of the GDPR which provides a framework for the recognition and enforcement of the fundamental right. This right/framework distinction is acknowledged within the GDPR at Article 1(2) where it acknowledges '[t]his Regulation ***protects*** fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'. The distinction between the roles of the Charter right and the GDPR is fine but important. The Charter (which holds treaty equivalence)[21] affords the right to data protection; the GDPR, which does not have treaty equivalence, is the framework to ensure this right is recognized and protected. Therefore it can clearly be argued that when the UK leaves the EU, and thereby the EU Charter, UK citizens (and EU citizens looking to enforce in the UK) will lose their *right* to data protection as found in Article 8 of the Charter. They will retain only the shadow of the right through the framework for data protection which will be found in the UK implementation of the GDPR. This essential distinction has a number of immediate implications. A domestic UK Data Protection Act cannot adequately replace the fundamental right to data protection found in the EU Charter. Such an Act, which is always subject to Parliamentary repeal, will only replicate the framework of data protection as found in the subordinate EU Legislation (the GDPR). Only if the UK Government were to adopt a right to data protection in some form in the proposed British Bill of Rights would there be true equivalence for Article 8 in domestic law. It may be argued that other UK international obligations such as Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its additional protocol[22] or the OECD Privacy Framework[23] could substitute for Article 8, but importantly for this analysis these international legal instruments do not hold the same constitutional status as the EU Charter both requiring domestic implementation.

This all becomes important when rights are thrown into conflict and domestic UK courts will become the final arbiter of data protection law in the UK.[24] As Advocate General Jääskinen demonstrated in *Google*

17 Department for Exiting the European Union, *Legislating for the United Kingdom's Withdrawal from the European Union*, Cm 9446, March 2017: [2.23] (emphasis added).

18 Ibid [2.25] (emphasis added).

19 Charter of Fundamental Rights of the European Union 2000/C 364/01, OJ 2012 C 326/391.

20 See also Cl.3(1) of the European Union (Withdrawal) Bill 2017–19: 'Direct EU legislation, so far as operative immediately before exit day, forms part of domestic law on and after exit day.'

21 Art 6(1), Treaty on European Union 2012/C 326/01, OJ 2012 C 326/3.

22 CETS 108, 28 January 1981 and ETS 181 8 November 2001.

23 <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> accessed 1 August 2017.

24 In this article, as in the Government White Paper, a UK Court, or UK Courts, should be interpreted as a Court or Courts of the constituent jurisdictions of the UK—ie England and Wales, Scotland or Northern Ireland.

Spain SL and another v Agencia Española de Protección de Datos and another,[25] there is a clear legal distinction between the Charter Right and the Directive (or Regulation) which gives effect to them.

> According to the ECHR and the Charter any interference to protected rights must be based on law and be necessary in a democratic society. In the present case we are not faced with interference by public authorities in need of justification but of the question of the extent that interference by private subjects can be tolerated. The limits to this are set out in the Directive, and they are thus based on law, as required by the ECHR and the Charter. ***Hence, when the Directive is interpreted, the exercise precisely concerns the interpretation of the limits set to data processing by private subjects in light of the Charter.***[26]

As will be argued below, this matters. There will no longer be a fundamental right to data protection in the UK post Brexit and this is something which cannot be remedied through domestic legal settlements short of a British Bill of Rights, and even then perhaps not so if Parliament retains sovereignty to amend or repeal these rights by normal Parliamentary procedures. This implies that EU27 citizens residing in the UK will not be able to rely on their Charter right, whereas EU27 citizens in EU27 Member States will be able to so do. This is more than a semantic difference as the UK seemingly seeks a hard Brexit beyond the jurisdiction of the ECJ and quite possible the EFTA Court.

It may be argued that this is moot due to the line of authority that may be drawn from *S and Marper v the United Kingdom*.[27] As was famously held in that case

> The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding. However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained.

This line of authority also encompasses *LH v Latvia*,[28] *Uzun v Germany*,[29] and earlier cases such as *X v Germany*.[30] This extensive definition of right to a private life clearly covers data privacy. Thus in *Marper*, the data in question were entries on the police database of a database of fingerprints, cell samples, and DNA profiles. In *LH* the data were personal medical data collected by the Inspectorate of Quality Control for Medical Care and Fitness for Work ('MADEKKI'). In *Uzun* the data were gathered as GPS data while in *X* the data were documents which had been photocopied in the applicant's office. Clearly, this line of authority suggests that the UK's failure to implement Article 8 of the EU Charter is less significant given the expansive interpretation the ECtHR has given to Article 8 of the ECHR for as long as the UK remains a member of the ECHR.

However, there are key differences between Article 8 of the EU Charter and Article 8 of the ECHR. By Article 8 of the EU Charter not only does the data subject retain the right to protection of personal data concerning him or her, they also are given a number of subsidiary rights which are not clearly given in Article 8 of the ECHR. Thus by Article 8 of the ECHR the only guarantees given to the data subject are that:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

This is very limiting for it is only interference by a public authority that engages the convention right.[31] The answer would appear to be the principle of horizontality, but as a number of authors, including Phillipson, have noted in determining horizontality: 'the issue appears to have been placed firmly in the keeping of the courts',[32] and recently in an Article 8 application in *McDonald v McDonald*[33] the Court of Appeal ruled that Article 8 does not have horizontal effect in the context of possession proceedings. This means that it is not clearly settled that the expansive definition of Article 8 ECHR would apply horizontally between private citizens in the UK legal systems. By comparison Article 8 of the EU Charter does have horizontal effect as afforded clearly by Article 8(2), and as recognized recently by the

25 Case C-131/12, 25 June 2013, ECLI:EU:C:2013:424 (AG Opinion) and 13 May 2014 ECLI:EU:C:2014:317 (Judgment) both reported at [2014] 3 CMLR 50.

26 Ibid [AG119] (emphasis added).

27 [2008] ECHR 1581.

28 [2014] ECHR 515.

29 [2011] 53 EHRR 24.

30 (8334/78) 7 May 1981. <http://hudoc.echr.coe.int/eng - {"appno": ["8334/78"]}> accessed 1 August 2017.

31 The author is acutely aware of significant commentary and case-law on the Horizontal Effect of the ECHR in UK law including Gavin Phillipson, 'The Human Rights Act, "Horizontal Effect" and the Common Law: a Bang or a Whimper?' (1999) 62 MLR 824 and Ian Loveland, 'Horizontality of Art 8 in the Context of Possession Proceedings' (2015) EHRLR 138. There is insufficient space here to discuss horizontality in full.

32 Phillipson, ibid 849.

33 [2014] EWCA Civ 1049.

Court of Appeal in *Vidal-Hall v Google Inc.*[34] Further Article 8 of the Charter gives two additional rights, the right to data access and rectification and the right to have reference to a supervisory authority. At risk of labouring the point, these rights will not be retained as *rights* post Brexit. The UK's data protection regime may be compliant but the right to data access and rectification and the right to have reference to a supervisory authority will be lost. Also lost will be the guarantee of horizontal effect and recognition. The existence of the expansive interpretation of Article 8 ECHR found in *Marper* and other cases is not a solution to this problem.

Despite the UK's continuing commitment, at least in the short term, to the ECHR it can therefore clearly be argued that a UK court will still not have the direct correspondent to Article 8 of the EU Charter in retained UK domestic law against which a court may interpret challenges to UK data protection law.[35] This is a position that may prove a happy resolution to some in the UK. As Mostyn J observed in the case of *AB*:[36]

> The claimant here asserts a violation of article 8 of the Charter of Fundamental Rights of the European Union. This right to protection of personal data is not part of the European Convention on Human Rights, and has therefore not been incorporated into our domestic law by the Human Rights Act. But by virtue of the decision of the court in Luxembourg, and notwithstanding the terms of the opt-out, the claimant is entitled, as Mr Westgate QC correctly says, surprising though it may seem, to assert a violation of it in these domestic proceedings before me.[37]

Against this backdrop, it almost seems an understatement to say, as Orla Lynskey does, 'the Charter has been accepted in the UK legal order only with great reluctance'.[38] This point was taken up by Marina Wheeler QC who noted that 'anxious that the Charter should not be used to overturn national law, the (then Labour) government negotiated what they believed to be an opt out of the Charter by means of Protocol No 30'[39] but that by 2013, and the *AB* decision, the position had been reversed such that as observed by Mostyn J 'that much wider Charter of Rights would remain part of our domestic law even if the Human Rights Act were repealed'.[40]

Ironically of course Brexit reverses this position and the UK finds itself divorced from the Charter but not from the ECHR. The importance of the Charter in UK Law as a source of fundamental rights, including the Article 8 right, may be seen in a number of cases including *Vidal Hall v Google*[41] and *Viagogo.*[42] This vital source of the fundamental data protection right is likely to be lost if the judgment in *AB* is to be followed. We could end up in a zero-sum game where as far as the UK Government is concerned, the equivalent of Article 8 is to be found in the UK implementing legislation giving effect to the GDPR, but where there is no Charter right with which to interpret obligations under the UK Legislation. The EU27 may see that as a failure to implement broadly equivalent protections for EU citizens.[43]

Further, a vitally important take-away from the *Google Spain* case is that interpretation of enabling frameworks within Charter rights may even extend our understanding of the enabling provisions. Advocate General Jääskinen believed that '[Article 8] being a restatement of the EU and Council of Europe acquis in this field, emphasises the importance of protection of personal data, but it does not as such add any significant new elements to the interpretation of the Directive'[44] leading him to conclude that 'The rights to erasure and blocking of data, provided for in Art.12(b), and the right to object, provided for in Art.14(a), of Directive 95/46, do not confer on the data subject a right to address himself to a search engine service provider in order to prevent indexing of the information relating to him'.[45] The Court though disagreed:

> The data subject may, in the light of his fundamental rights under Arts 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic

34 [2015] EWCA Civ 311.

35 See further cl.6(3) of the European Union (Withdrawal) Bill 2017–19: 'Any question as to the validity, meaning or effect of any retained EU law is to be decided, so far as that law is unmodified on or after exit day and so far as they are relevant to it— (a) in accordance with *any retained case law and any retained general principles of EU law*' (emphasis added).

36 *AB, R (on the application of) v Secretary of State for the Home Department* [2013] EWHC 3453.

37 Ibid [16].

38 Orla Lynskey, 'Courts, Privacy and Data Protection in the UK: Why Two Wrongs don't Make a Right' in M Brkan and E Psychogiopou (eds), *Courts, Privacy and Data Protection in the Digital Environment* (2017) 215, 229.

39 Marina Wheeler, 'Cavalier with our Constitution: a Charter too Far', *UK Human Rights Blog*, 1 Crown Office Row (9 February 2016) <https://ukhumanrightsblog.com/2016/02/09/cavalier-with-our-constitution-a-charter-too-far/> 22 May 2017.

40 Above n 36, [14].

41 Above n 34.

42 *The Rugby Football Union v Consolidated Information Services Ltd* [2012] UKSC 55.

43 At this point it may be further noted that even if one were to accept the expansive interpretation of art 8 ECHR as being equivalent to art 8 of the Charter there would be less strong enforceability and a less effective remedy available under the ECHR than under the Charter.

44 Above n 25, [AG113].

45 Ibid [AG138(3)].

> interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name.[46]

The essential difference in Advocate General Jääskinen's approach and that of the Court is the Court's willingness to interpret the Directive expansively in light of Charter rights, including Article 8, which they see as overriding. A UK court post-Brexit (assuming there is to be no 'right' to data protection implemented elsewhere) would be unable to do so. This returns us to Baroness Janke's question and Recital 41. It will in all likelihood be impossible for a domestic UK court to interpret 'a legal basis or a legislative measure . . . in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights' where the fundamental Right to Data Protection found in Article 8 is in question for there will be no domestic equivalent. This appears to be the case due to the current wording of cl.6(3)(a) of the European Union (Withdrawal) Bill (subject to amendment). There it states that in interpreting retained EU Law any court or tribunal must decide the validity, meaning or effect of any retained EU law 'so far as that law is unmodified on or after exit day and so far as they are relevant to it *in accordance with any retained case law and any retained general principles of EU law*' (emphasis added). As, as has been previously argued, there will be no retention of Article 8 of the EU Charter they will not be able to refer to Article 8 as it is not a 'retained general principle of EU law'.

GDPR and adequacy

The UK Government seems to be of the opinion that as part of the Article 50 negotiations the EU27 will recognize the UK implementation of the GDPR (and related provisions including the Law Enforcement Directive[47]) as being suitable for an adequacy decision under Article 45 GDPR or some form of equivalent measure adopted as part of a bilateral treaty or agreement negotiated as part of the Article 50 process. As noted above, the Government is quite coy on how this might be achieved with the Minister of State for Digital and Culture refusing to be drawn on whether an adequacy decision was necessary. This seems to suggest the UK will seek to negotiate this as part of the Article 50 settlement.

While we are somewhat in uncharted waters with the Article 50 process which rather baldly states 'the Union shall negotiate and conclude an agreement with that State, setting out the arrangements for its withdrawal, taking account of the framework for its future relationship with the Union', what is clear though is that the EU27 cannot agree to anything which would be against EU Law as part of the Article 50 settlement with the UK. The agreement itself, as a new International Treaty enacted by the EU Institutions, would be subject to a possible legality challenge before the ECJ in so far as the EU Institutions cannot act in a way that breaches primary law, including the Charter.[48] This position has recently been confirmed by the CJEU in the *Opinion 1/15* judgment.[49] This judgment is instructive in several ways to this analysis. First it confirms that in place of an adequacy decision, the European Union may enter into an international agreement with a third country which allows for the exportation of data to that third country.[50] However, and vital to the current analysis, the Court found that any independently negotiated agreement (as under Article 50) must meet the same adequacy standards as Article 45 agreements.[51] Perhaps equally as importantly the Court reminded us that where data are transferred to a third country, whether under an Article 45 adequacy ruling or under an independently negotiated agreement the third country must also take steps to prevent exportation of that data to countries which fail to provide EU level protection to the personal data.[52]

Legally post Brexit the UK will be classified as a 'third country' in GDPR terms, whether or not an agreement for data transfers is negotiated as an adequacy decision or as an independent agreement as part of the Article 50 negotiations. The impact of this is that any agreement, whether negotiated as part of the Article 50 settlement or separately must according to the decisions in both

46 Ibid [99].

47 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 2016 L 119/89.

48 Case C–402/05 P and C–415/05, *Kadi and Al Barakaat International Foundation v Council and Commission* 3 September 2008, ECLI:EU:C:2008:461, [2008] ECR I–6351.

49 Opinion procedure 1/15, Request for an Opinion pursuant to Article 218(11) TFEU, made on 30 January 2015 by the European Parliament, 26 July2017, ECLI:EU:C:2017:592.

50 At [214] the Court concludes that "disclosure requires the existence of either an agreement between the European Union and the non-member country concerned equivalent to that agreement, or a decision of the Commission, under Article 25(6) of Directive 95/46, finding that the third country ensures an adequate level of protection within the meaning of EU law and covering the authorities to which it is intended PNR data be transferred".

51 Ibid [67]. Further at [214] the Court notes that "a transfer of personal data from the European Union to a non-member country may take place only if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union".

52 Ibid [134], [214].

Kadi and *Opinion 1/15* meet existing EU legal standards and frameworks. This means that any agreement entered into by the UK Government and the EU27 Member States will need to comply with Chapter V/ Article 44 of the GDPR.

Assuming the UK will not be an EEA state, a position held by the UK Government,[53] then transfers to the UK from the EEA post-Brexit will need to be authorized by one of the suite of available GDPR options. The most likely outcome is an Article 50 treaty or settlement agreed under the same legal framework as the GDPR. Alternatives include a stand-alone adequacy ruling under Article 45, or that transfers be permitted subject to safeguards under Article 46, or be made subject to Binding Corporate Rules under Article 47. These seem to be the only options, as derogations under Article 49 could not apply in all cases. Of the remaining GDPR-compliant provisions (remembering that applying the decisions of the Court in *Kadi* and *Opinion 1/15* agreements made as part of the Article 50 negotiations would need to be GDPR compliant)[54] we find that Article 47 does not create a blanket right for 'the unhindered flow of data between the UK and the EU' that the UK Government is seeking so it seems it can be discounted. This leaves two options 'transfers subject to appropriate safeguards' under Article 46 or 'transfers on the basis of an adequacy decision' under Article 45.

If the UK believes that an adequacy decision may not be required then this may suggest that the Government believes that transfers may take place under some form of master agreement under Article 46. This provides that 'a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available'. A safeguards settlement though could not possibly be negotiated during Article 50 negotiations as the undertaking must be given by the controller or processor and cannot be given by the supervisory authority. Although supervisory authorities may authorize standard data protection clauses or approved codes of conduct, agreement would have to be reached individually with data controllers or processors. This means Article 46 cannot be employed to achieve the Government's aims.

We are therefore by process of elimination left with Article 45 either as a stand-alone adequacy decision, or some form of equivalent adequacy settlement independently negotiated under the Article 50 process. The UK Government seems though unwilling to acknowledge this publicly. From the current mood in Westminster it may be assumed that the Government is seeking to put in place an adequacy-equivalent decision as part of the Article 50 negotiations. In fact it may be argued that this position has been publicly acknowledged in the Article 50 letter itself. There the Prime Minister wrote: 'leading in the world, and defending itself from security threats . . . . We therefore believe it is necessary to agree the terms of our future partnership alongside those of our withdrawal from the European Union.'[55] This is clearly a (not very) veiled reference to the UK's excellence in signals intelligence (SIGINT) data gathering and the need to share data for law enforcement purposes, a point she returned to later in the letter saying, 'in security terms a failure to reach agreement would mean our cooperation in the fight against crime and terrorism would be weakened'.[56] It seems a data sharing agreement, which one imagines would include an adequacy decision, is explicitly going to be part of the Article 50 negotiations. As a result it may be concluded that the UK is seeking to enter into an independent agreement with the EU27 Member States to allow for the free flow of data post Brexit. Such agreement will be required to be in compliance with Article 45 principles for the reasons set out in *Opinion 1/15*.

What will a UK adequacy-standard agreement look like though? At first glance it would seem pretty straightforward, for as Baroness Williams suggests, 'on the day that we leave our laws are compatible with those of the EU';[57] however, as we have seen subsequently this is not the case both institutionally and constitutionally. The CJEU will no longer have authority over the domestic UK legal settlement, the EU Charter, and in particular Article 8, will have no direct equivalent in UK law and the 105 references to the Commission will have been excised from (or will be meaningless in) the UK legislation giving effect to GDPR, and the UK will be

53 A UK Government Spokesperson is recorded as saying "The UK is party to the EEA agreement only in its capacity as an EU member state. Once the UK leaves the EU, the EEA agreement will automatically cease to apply to the UK" in L Hughes and J Eysenck, 'What is the new article 127 Brexit challenge – and what does it mean?' *Daily Telegraph* (2 February 2017) <http://www.telegraph.co.uk/news/0/article-127-new-brexit-legal-challenge-single-market/> accessed 1 August 2017.

54 Above n 48 and n 51.

55 Prime Minister's letter to Donald Tusk triggering Article 50 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/604079/Prime_Ministers_letter_to_European_Council_President_Donald_Tusk.pdf> accessed 1 August 2017.

56 Ibid.

57 Above n 5.

withdrawn from the EDPB. In short it is far from as simple as Baroness Williams suggests.

Happily, the UK's implementation of GDPR and related Directives will ensure that the UK will meet most, if not all, Article 45 requirements on day one. It will possess clearly an effective supervisory authority in the form of the Information Commissioner's Office, which will have equivalent powers and responsibilities to other EU27/EEA supervisory authorities. It will have similar international commitments to its EU27/EEA partners and will still, at least at the outset, be party to the ECHR; the leading regional system for the protection of privacy aspects of personal data. The UK will possess the necessary legal framework for the recognition of the rights of data subjects and will have an effective and functioning system for effective and enforceable administrative and judicial redress for the data subjects whose personal data are being transferred. When one compares, for example, the position of the UK on 29 March 2019 with the position of a number of countries which have adequacy decisions such as Switzerland, Uruguay or the Privacy Shield agreement with the Federal Government of the USA it is clear the UK will have a much more comprehensive and compliant data protection regime. The UK should therefore qualify immediately for an adequacy-standard agreement. However, there is one UK legal provision which may prove problematic both in the short-term and in the longer term.

The investigatory powers act 2016

The Investigatory Powers Act 2016 is a comprehensive restatement of UK security and intelligence laws. It covers a variety of law enforcement and investigatory techniques employed by the police and by the security and intelligence services from interception of communications to equipment interference and covers a wide range of targeted and bulk warrants.

For the purposes of this article, we will focus on Part 4: Retention of Communications Data. This part of the Act permits data retention orders to be issued, replacing the provisions of the now repealed Data Retention and Investigatory Powers Act 2014 (DRIPA). The effective power is found in section 87(1). This permits the 'Secretary of State [to] require a telecommunications operator to retain relevant communications data if (a) the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (j) of section 61(7) (purposes for which communications data may be obtained), and (b) the decision to give the notice has been approved by a Judicial Commissioner'. The key difference between s.87(1) and s.1(1) of DRIPA is the addition of sub-section (b): oversight by a Judicial Commissioner. The list of permitted purposes found in section 61(7) is at first glance wider than that permitted under DRIPA. New permitted purposes include: (i) to assist investigations into alleged miscarriages of justice; (ii) to assist in the identification of a person or their next of kin; and (iii) functions relating to the regulation of financial services and markets, or financial stability. Some purposes have been removed or narrowed, offsetting some of the new purposes. Thus, the previously permitted purpose of 'in the interests of the economic well-being of the United Kingdom' has been narrowed by the addition of qualifying text 'so far as those interests are also relevant to the interests of national security' while a general law-making power 'for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State' is removed. This final amendment, alongside the role of the Judicial Commissioners may assist the UK Government in securing an adequacy decision, although as we shall see this is far from certain.

Significant new safeguards have been added. By section 88 the Secretary of State must take a reflective overview of the need to issue a retention notice before it is issued taking into account (among others): the likely benefits of the notice, the likely number of users (if known) of any telecommunications service to which the notice relates, the technical feasibility of complying with the notice, and the likely cost of complying with the notice. Further by section 88(2) the Secretary of State must, before giving such a notice, take reasonable steps to consult any operator to whom it relates. The second additional safeguard is the addition of the review of the Judicial Commissioners. The role of the Judicial Commissioners is new and may be found in section 227. This creates the new positions of the Investigatory Powers Commissioner and other Judicial Commissioners. The Investigatory Powers Commissioner is the chief Judicial Commissioner and must have held high judicial office (as must the other Judicial Commissioners). Lord Justice Fulford, Senior Presiding Judge for England and Wales, has been appointed as the first Investigatory Powers Commissioner.[58] The Judicial Commissioners are charged under section 89(1) to 'review the Secretary of State's conclusions as to whether the requirement to be imposed by the notice to retain relevant communications data is necessary and

58 Her Majesty's Government, *Press Release Investigatory Powers Commissioner Appointed: Lord Justice Fulford*, 3 March 2017. <https://www.gov.uk/government/news/investigatory-powers-commissioner-appointed-lord-justice-fulford> accessed 1 August 2017.

proportionate for one or more of the purposes falling within paragraphs (a) to (j) of section 61(7)'. However the way they are to do this is rather unusual. By section 89(2)(a) they are directed to 'apply the same principles as would be applied by a court on an application for judicial review' while by section 89(2)(b) they are required to 'consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy)'.

These two provisions seem to be in conflict. The duties imposed by section 2 ask the Commissioners to weigh: (i) whether what is sought to be achieved by the warrant, authorization or notice could reasonably be achieved by other less intrusive means; (ii) whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of that information; (iii) the public interest in the integrity and security of telecommunication systems and postal services; and (iv) any other aspects of the public interest in the protection of privacy against (a) the interests of national security or of the economic well-being of the UK, and (b) the public interest in preventing or detecting serious crime. However, this solemn weighting of privacy against the public interest is somewhat undermined by the section 89(2)(a) requirement that the Judicial Commissioners 'apply the same principles as would be applied by a court on an application for judicial review'.

Judicial review principles are rather narrow and review the administrative process of the decision rather than the substance of the decision. This means commissioners will be restricted in the scope of their actions to the three Judicial Review grounds: (i) Illegality: conflict with legal order or *ultra vires*; (ii) Fairness: a public body should never act so unfairly that it amounts to an abuse of power; and (iii) Irrationality and proportionality: a decision may be considered so demonstrably unreasonable as to constitute 'irrationality' or 'perversity' on the part of the decision maker.

Some have criticized the adoption of judicial review principles. Appearing before the Joint Committee on the Draft Investigatory Powers Bill Caroline Wilson Palow, General Counsel of Privacy International, argued that 'the Judicial Commissioners need the full ability to assess the warrants when they come to them. It should not be just a judicial review standard. They need to assess fully the substance of the warrant and, among other things, whether there are other less obtrusive means by which this information could be obtained'.[59] Shami Chakrabarti, then Director of Liberty, was more forceful.

> Judicial review does not help at all in this context. When you are deciding whether it is proportionate to issue a warrant for intrusive surveillance of an individual, let alone of a whole group of people, that is a judgment made on the evidence. A judicial review test only second-guesses the Secretary of State, in very limited circumstances. Did they make a bonkers decision that no reasonable Secretary of State could take?[60]

Others take a more sympathetic view to the use of Judicial Review standards. Lord David Pannick QC in an article for *The Times* newspaper noted that 'Andy Burnham and David Davis . . . say that a judicial review test gives judges too little power because it only relates to 'process'. But it is well established that judicial review is a flexible concept, the rigour of which depends on the context. The Court of Appeal so stated in 2008 in the T-Mobile case'.[61] He goes on to point out that Judges already apply Judicial Review standards successfully in a complex rights framework.

> [t]he closest analogy to the provisions in the draft bill is judicial review of control orders and Tpims (terrorist prevention and investigation measures). The Court of Appeal stated in the MB case in 2006 that judges applying a judicial review test must themselves consider the merits and decide whether the measure is indeed necessary and proportionate. It is true that the context there involves restrictions that vitally affect liberty — in the sense of freedom of movement. But I would expect the courts to apply a very similar approach in the present context, concerned as it is with the important issue of privacy. So those who are concerned that a judicial review test does not give judges sufficient control should be reassured.[62]

Sir Stanley Burnton, then Interception of Communications Commissioner, and Lord Judge, then Chief Surveillance Commissioner, both endorsed the Pannick approach, however not without reservation. In their evidence to the Joint Committee on the Draft Investigatory Powers Bill Sir Stanley noted that 'Judicial review is not simply a question of looking at process. [T]he commissioner has to look at necessity and proportionality. The degree to which judicial review is imposed as a test and

59 Joint Committee on the Draft Investigatory Powers Bill, Oral evidence: Draft Investigatory Powers Bill, HC 651, Wednesday 9 December 2015 <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/oral/25977.html> accessed 1 August 2017.

60 Ibid.

61 David Pannick QC: 'Safeguards Provide a Fair Balance on Surveillance Powers', *The Times* (12 November 2015). The T-Mobile case refereed to is *T-Mobile & Telefonica v Ofcom* [2008] EWCA Civ 1373.

62 Ibid.

the stringency of the test depend very much on the context, the facts of the individual case and the consequences of the administrative or governmental decision in question'.[63] Lord Judge supported Sir Stanley's position but added a hesitation.

> My only hesitation, which is a lawyerly one but not totally without some force, is in using the words 'judicial review' as a description of the test that has to be applied by the judicial officer. Judicial review used to be Wednesbury unreasonable mad. We would call it Wednesbury unreasonable, meaning only an idiot could have reached this decision. Nowadays, judicial review is less stringent than that: 'He is not an idiot, but it is a really stupid decision'. That is not quite the same. 'I am not sure many people would have reached this decision' is another test. We need to be slightly careful. If you are talking about the Home Secretary ... [t]he Home Secretary has the most amazing responsibilities in relation to that. Judges second guessing is simply inappropriate. You have to have a stringent judicial review test. I am now coming back to what Sir Stanley said. You know you are dealing with national security; you know somebody might be planting a bomb. You are going to be very cautious about interfering and saying, 'This man or woman, who is the Secretary of State, is daft'.[64]

Lord Judge's hesitation raises a note of concern that may impact the UK's ability to obtain an equivalency decision. The draft of the Bill being discussed in Committee on that date did not contain a provision equivalent to section 89(2)(b). Some may argue the addition of section 89(2)(b) will empower Judicial Commissioners to take the expansive Pannick view that will employ 'a judicial review test [which] must [] consider the merits and decide whether the measure is indeed necessary and proportionate' however if as he says 'judicial review is a flexible concept, the rigour of which depends on the context' then the risk is that when s.89(2)(a) and 89(2)(b) are placed in conflict Judicial Commissioners will follow the Judge line that warrants should only be refused when the Commissioner believes that 'this man or woman, who is the Secretary of State, is daft'. This could have far-reaching implications for the recognition of adequacy in UK data protection law post Brexit due to the line of authority of *Digital Rights Ireland Ltd v Minister for Communications*,[65] *Maximillian Schrems v Data Protection Commissioner*,[66] and *Tele2 Sverige AB v Post-och telestyrelsen*.[67]

Digital Rights Ireland ltd v minister for communications[68]

The *Digital Rights Ireland* case was, of course, was the famous challenge to the now repealed Data Retention Directive.[69] While the long-term legal impact of the case is reduced due to the fact that it was a specific challenge to the Directive's legality there are still a number of important take-aways for a post-Brexit data protection environment.

While much of the detail of the case turned upon the interplay between Article 15(1) of the ePrivacy Directive,[70] Article 13(1) of the Data Protection Directive[71] and the provisions of the Data Retention Directive,[72] there were elements of interplay also with the EU Charter and the rights framework of the EU. Vitally the Court found

> The retention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. ***Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article***.[73]

This is important as it confirms that data retention processes engage Article 8 of the EU Charter and as we have seen above Article 8 is one of the provisions of the Charter not to have guaranteed recognition in the UK in the post-Brexit environment. Now, as we have already rehearsed, an argument may be made that by importing the GDPR framework into domestic UK law in full then the UK will have satisfied 'the data protection

63 Joint Committee on the Draft Investigatory Powers Bill, Oral evidence: Draft Investigatory Powers Bill, HC 651, Wednesday 2 December 2015 <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/oral/25685.html> accessed 1 August 2017.

64 Ibid.

65 Joined Cases C–293/12 and C–594/12, 8 April 2014, ECLI:EU:C:2014:238.

66 Case C–362/14, 6 October 2015, ECLI:EU:C:2015:650.

67 Joined Cases C–203/15 and C–698/15, 21 December 2016, ECLI:EU:C:2016:970.

68 Above n 65.

69 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 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 2006 L 105/54.

70 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L 201/37.

71 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 2005 L 281/31.

72 Above n 69.

73 *Digital Rights Ireland Ltd v Minister for Communications*, above n 65, [29] (emphasis added).

requirements arising from that article'. However a contrary interpretation is that, again as we have seen, when the UK leaves the EU, UK citizens (and EU citizens looking to enforce in the UK) will lose their right to data protection as found in Article 8. They will, as set out above, retain only the shadow of the right through the framework for data protection found in the UK implementation of the GDPR.

In *Digital Rights Ireland* the court found that 'Directive 2006/24 constitutes an *interference* with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data'.[74] This is an important development. The Court clearly states that data retention not only engages Article 8, it is also an interference with the fundamental right to data protection. The question then comes down to whether or not that interference is justified. After quickly finding that 'the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest'[75] that interest being 'the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest and the fight against serious crime in order to ensure public security'[76] the Court moved on to the question of proportionality.

Here the Court found that 'in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict'.[77] The Court further noted, 'the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter'.[78] As a result of this 'the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data'.[79] Finding that the Directive required all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony to be retained the Court found the Directive not to be a proportionate response to the threat and struck it down. In so doing the Court ruled:

> Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality.[80]

The risk of this decision to the post-Brexit flow of data between the EU27/EEA and the UK is clear. The Investigatory Powers Act does not have these protections. Section 2, as implemented in data retention cases by section 89(2)(b), asks the Judicial Commissioners to consider 'whether what is sought to be achieved by the warrant, authorisation or notice could reasonably be achieved by other less intrusive means' and 'whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of that information'. In addition by section 92 'a telecommunications operator who retains relevant communications data must (a) secure that the data is of the same integrity, and subject to at least the same security and protection, as the data on any system from which it is derived, (b) secure, by appropriate technical and organisational measures, that the data can be accessed only by specially authorised personnel, and (c) protect, by appropriate technical and organisational measures, the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure'. The Government believes that collectively these represent implementation of data protection provisions for retained data. Essentially if the system was data protection compliant when the data were gathered then it will remain so under section 92(1)(a) while retained. However there are two problems with this. The first is that this appears to be far short of 'govern[ing] the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity

74 Ibid [36] (emphasis added).
75 Ibid [44].
76 Ibid [42].
77 Ibid [48].
78 Ibid [53].
79 Ibid [54].
80 Ibid [66].

and confidentiality'. The second is that it assumes the data retained were in a compliant system at the point it was retained. Currently, this would be subject to a challenge that engages Article 8 of the EU Charter. Post-Brexit this will not be possible.

Tele2 sverige ab v post-och telestyrelsen

Two UK MPs, David Davis MP (now ironically Secretary of State for Exiting the EU) and Tom Watson MP brought a challenge to the UK's subsequent domestic legislation, the Data Retention and Investigatory Powers Act 2016 (DRIPA). The reference to the CJEU from the UK Court of Appeal was joined with a Swedish reference *Tele2 Sverige AB v Post-och telestyrelsen*.[81] Davis and Watson (later just Watson as Davis's appointment to the UK Cabinet placed him in conflict and he was required to drop out of the challenge) argued that the Digital Rights Ireland judgment laid down 'mandatory requirements of EU law' applicable to the legislation of Member States on the retention of communications data and access to such data. This meant that the provisions of DRIPA, which broadly replicated the provisions of the Data Retention Directive (though subject to a 'retention notice' issued under section 1(1) by the Secretary of State rather than as a blanket retention as the Directive had provided), were unlawful under EU law. The Divisional Court agreed finding that as the Data Retention Directive was incompatible with the principle of proportionality, national legislation containing the same provisions as that Directive could, equally, not be compatible with that principle.[82] The Government appealed and the Court of Appeal took a different interpretation taking a provisional view that, in *Digital Rights Ireland*, the Court of Justice was not laying down specific mandatory requirements of EU law with which national legislation must comply, but was simply identifying and describing protections that were absent from the harmonized EU regime, while referring the case to the CJEU.[83]

The Court of Appeal referred two questions to the CJEU:

1. Did the CJEU in Digital Rights Ireland intend to lay down mandatory requirements of EU law with which the national legislation of Member States must comply?
2. Did the CJEU in Digital Rights Ireland intend to expand the effect of Articles 7 and/or 8, EU Charter beyond the effect of Article 8 ECHR as established in the jurisprudence of the ECtHR?[84]

When the cases were joined, the CJEU slightly altered the approach to the questions but the key questions of whether the *Digital Rights Ireland* case laid requirements on Member States, and what the correct approach to the application of Articles 7 and 8 were, remained.

Like the *Digital Rights Ireland* case much of the discussion both in Advocate General Saugmandsgaard Øe's and in the Court's opinion turned on technical issues of the interplay of the EU legal framework. The key question here was whether the existence of the data retention provision found in Article 15(1) of the ePrivacy Directive precluded Member States from making domestic legislation in this area without reference to Article 15(1). As such the argument of the claimants was that domestic legislation made under Article 15(1) would be bound by the principles of Digital Rights Ireland. This is a very interesting and important point but not directly relevant to this analysis so will not be pursued further here.[85]

Essential to our analysis here is the interplay between the domestic UK legislation and the UK's responsibilities under the EU Charter. A key point raised by Advocate General Saugmandsgaard Øe in relation to domestic regimes as opposed to a harmonized one, was:

> In accordance with Art.8(3) of the Charter, every Member State must ensure that an independent authority reviews compliance with the requirements of protection and security on the part of the service providers to which their national regimes apply. In the absence of coordination throughout the European Union, however, those national authorities might find it impossible to fulfil their supervisory duties in other Member States.[86]

This is a question likely to be magnified post-Brexit when the UK leaves the EU Charter. In his analysis of whether the Swedish and UK provisions met the requirements of Articles 7 & 8 of the Charter Advocate General Saugmandsgaard Øe observed that an argument made by the UK Government that 'a general data

81 Above n 67.

82 *R v Secretary of State for the Home Department (ex parte Davis & Watson)* [2015] EWHC 2092 (Admin).

83 *Secretary of State for the Home Department v Davis and Ors* [2015]. EWCA Civ 1185.

84 Ibid [118].

85 Although not relevant to this analysis, this point is very important for the Brexit position of the Investigatory Powers Tribunal (IPT). If the IPT upholds this point they may find that the EU did not have competence to act in national security matters and post Brexit any EU provisions are inapplicable. This in itself is not an issue for an equivalence decision as art 23(1)(a)of the GDPR allows for restrictions. This matter was discussed in *Secretary of State for the Home Department v Davis and Ors*, above n 83, at [91]–[106].

86 Opinion of Advocate General Saugmandsgaard Øe delivered on 19 July 2016 in *Tele2 Sverige AB v Post-och telestyrelsen* (C–203/15) and *Secretary of State for the Home Department v Tom Watson* (C–698/15) ECLI:EU:C:2016:572 at [241].

retention obligation may be justified by any of the objectives mentioned in either Art.15(1) of Directive 2002/58 or Art.13(1) of Directive 95/46. According to that such an obligation could be justified by the utility of retained data in combating 'ordinary' (as opposed to 'serious') offences, or even in proceedings other than criminal proceedings, with regard to the objectives mentioned in those provisions'[87] was 'not convincing'. He came to this conclusion for several reasons but prime among them was

> The requirement of proportionality within a democratic society prevents the combating of ordinary offences and the smooth conduct of proceedings other than criminal proceedings from constituting justifications for a general data retention obligation. The considerable risks that such obligations entail outweigh the benefits they offer in combating ordinary offences and in the conduct of proceedings other than criminal proceedings.[88]

The CJEU in their judgment backed Advocate General Saugmandsgaard Øe's interpretation finding that 'the objective pursued by that legislation must be proportionate to the seriousness of the interference in fundamental rights that that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting ***serious*** crime is capable of justifying such access to the retained data'.[89]

This remains a problem for the UK Government. By section 87(1) of the Investigatory Powers Act 2016 the Secretary of State may issue a retention notice if the Secretary of State 'considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (j) of section 61(7)'. These purposes are: (i) the interests of national security; (ii) preventing or detecting crime or of preventing disorder; (iii) the economic well-being of the UK so far as those interests are also relevant to the interests of national security; (iv) in the interests of public safety; (v) for the purpose of protecting public health; (vi) for assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; (vii) for preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; (viii) to assist investigations into alleged miscarriages of justice; (ix) where a person has died or is unable to identify themselves because of a physical or mental condition to assist in identifying them, or to obtain information about their next of kin or other persons connected with them; (x) for the purpose of exercising functions relating to the regulation of financial services and markets, or financial stability.

Looking at this list only (i), (iii) and (iv) seem clearly to meet the standard the Court is thinking of. It is possible in certain circumstances that (ii) (v) and (x) are compliant, but it is hard to think of cases where (vi), (vii), (viii) and (ix) would meet the high *Tele2* standard. Most clearly heading (ii) preventing or detecting crime or of preventing disorder does not meet the *Tele2* standard that 'only the objective of fighting ***serious*** crime is capable of justifying such access to the retained data'.

Additionally, the Investigatory Powers Act retains the wide scope of the DRIPA provision, what may be called a 'general or indiscriminate' notice. By section 87(2)(a)–(c) a retention notice may 'relate to a particular operator or any description of operators', 'require the retention ***of all data or any description of data***', and 'identify the period or periods for which data is to be retained' (emphasis added). Collectively, these provisions suggest notices which can apply to a particular operator (or a number of operators), may be defined so as to retain all data that operator holds for an extended period. This fits the definition of a 'general or indiscriminate' notice that the Court ruled to be incompatible with the Charter in *Tele2*.[90] This suggests a fundamental difference in approach between the UK and the EU27 on this matter.

It is not only the question of purposes which may affect the UK's ability to obtain an adequacy decision post *Tele2*. The question of the UK's supervisory arrangements for retention orders under Part 4 is also questionable. *Tele2* requires:

> Member States [to] ensure review, by an independent authority, of compliance with the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data, that control being expressly required by Art.8(3) of the Charter and constituting, in accordance with the Court's settled case-law, an essential element of respect for the protection of individuals in relation to the processing of personal data. If that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data.[91]

87 Ibid [169].

88 Ibid [172].

89 *Tele2 Sverige AB v Post-och telestyrelsen* (C–203/15) and *Secretary of State for the Home Department v Tom Watson* (C–698/15) above n 67 at [115] (emphasis added).

90 Ibid [103], [112].

91 Ibid [123].

The UK meets this in the Investigatory Powers Act 2016 through section 244: 'The Information Commissioner must audit compliance with requirements or restrictions imposed by virtue of Part 4 in relation to the integrity, security or destruction of data retained by virtue of that Part.' However, it is certainly not clear that this simple audit role meets the requirement of *Tele2* that 'persons have a right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data'. Individuals who wish to challenge the retention and storage of personal data under a data retention notice must do so through an application to the Investigatory Powers Tribunal (discussed further below). This may only be done in accordance with section 65 of the Regulation of Investigatory Powers Act 2000. This allows for two forms of challenge: a claim under the Human Rights Act 1998 for any breach of fundamental rights; or a complaint against a public authority for using covert techniques. Although providing a remedy, and arguably as will be discussed below, one which is probably GDPR complaint, this is a judicial procedure and seems quite distinct from the role of national supervisory authorities as required by *Tele2*.

In short, there are a number of areas where the interaction of the Investigatory Powers Act 2016 and the decision in *Tele2* may find themselves in conflict. These all potentially undermine the UK's ability to receive an adequacy decision under Article 45 GDPR.

Schrems

Inevitably when discussing the interplay between data transfers and adequacy decisions one finds himself faced with the *Schrems* decision.[92] This was the famous challenge to the Safe Harbor adequacy decision[93] brought by Austrian student Max Schrems following the Snowden revelations. Mr Schrems argued, ultimately successfully, that 'that the law and practices of the United States offer no real protection of the data kept in the United States against State surveillance'.[94]

The potential parallels between the *Schrems* challenge and the UK's desire to have an adequacy ruling post-Brexit are clear. The UK, like the USA, operates a massive state surveillance regime involving not only data retention as this article has discussed at length, but also policies such as TEMPORA, the system used by GCHQ to buffer most Internet communications extracted from fibre-optic cables so these can be processed and searched at a later time. This programme is operated alongside commercial partners such as Vodafone and British Telecommunications making it not unlike the PRISM programme at the heart of the Schrems case.

The key question is, given the previous discussion of the UK's data retention programme, and the decisions in *Digital Rights Ireland* and *Tele2*, could *Schrems* deliver a potentially fatal blow to any attempts by the UK Government to secure a lasting adequacy ruling in the Article 50 negotiations?

The first thing to note is that by implementing the GDPR in full and given the pre-existence of a supervisory authority in the form of the Information Commissioner's Office the UK sidesteps the main complaint in *Schrems*: the UK has a functional and functioning out of court dispute resolution system operated by an independent third party. However, the role of the Information Commissioner's Office is limited in questions of national security.[95] We can assume that in any domestic legislation giving effect to the GDPR the UK Government will seek to continue the exemption the security services currently enjoy through an implementation of the Article 23 GDPR restriction. Currently, the UK is shielded from any implication of this restriction by the fact that it is an EU Member State and subject to effective supervision via the CJEU with the full force of EU law, including the Charter, in place. When the UK leaves and goes alone it loses this framework. The Commission in coming to an adequacy decision will be required to apply *Schrems* and this tells us that 'legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Art.47 of the Charter'.[96] In the *Schrems* case there was insufficient protection of Article 47 for in the words of Advocate General Bot 'there is oversight on the part of the FISC, but the proceedings before it are secret and ex parte. I consider that that amounts to an interference with the right of citizens of the Union to an effective remedy, protected by Art.47 of the Charter'.[97]

Under the Investigatory Powers Act 2016 and the Regulation of Investigatory Powers Act 2000 the only

92 *Maximillian Schrems v Data Protection Commissioner*, above n 66.

93 European Commission Decision 2000/520 of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000 L215/7.

94 Opinion of Advocate General Bot delivered on 23 September 2015, Case C–362/14, ECLI:EU:C:2015:627 *Maximillian Schrems v Data Protection Commissioner*, [AG25].

95 See s 28 of the Data Protection Act 1998.

96 Above n 66, [95].

97 Above n 94, [173].

effective route to challenge any decision or action of the security services is the Investigatory Powers Tribunal. The Tribunal is not unlike FISC in that by section 68 of the Regulation of Investigatory Powers Act 2000 it may 'determine their own procedure in relation to any proceedings, complaint or reference brought before or made to them'. In practice procedure is as stated on the Tribunal's web site.

> We are the first court of our kind to establish 'inter partes' hearings in open court in the security field. These hearings allow us to hear arguments on both sides on the basis of 'assumed facts' without risk to our national security. This means that where there is a substantial issue of law to consider, and without at that stage taking a decision as to whether the allegation in a complaint is true, we invite the parties involved to present issues of law for the Tribunal to decide, which are based on the assumption that the facts alleged in the complaint are true. This means that we have been able to hold hearings in public, including full adversarial argument, as to whether the conduct alleged, if it had occurred, would have been lawful. We may then hold 'closed' hearings in private to apply the legal conclusions from the open hearings to the facts.[98]

This mixture of open inter partes hearings and then closed hearings on the facts may be enough to allow the UK to convincingly argue that the IPT is quite distinct from FISC and therefore the UK is compliant with Article 47.

The story does not end there though. Perhaps the key outcome of *Schrems* was the clear statement that 'legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter'.[99] Again the UK has until now been shielded by its EU membership and in particular its membership of the Charter. This time the UK may point to the fact that it remains an ECHR state (at least for the foreseeable future) and as a result for Article 7 of the Charter we may substitute Article 8 ECHR. However it is clear that the Investigatory Powers Act 2016 contains a number of provisions that apply to EU27 residents and citizens in a different manner to 'individuals in the British Islands'.[100] For example if one looks to section 136, Bulk Interception Warrants we are told that they may only be issued for 'the interception of overseas-related communications' and that this is 'communications sent by individuals who are outside the British Islands, or communications received by individuals who are outside the British Islands'. Similar distinctions may be found in section 158 (Bulk Acquisition Warrants) and section 176 (Bulk Equipment Interference Warrants).[101]

Thus EU27 residents (and presumably overwhelmingly citizens) in the UK will be treated differently under the Investigatory Powers Act to UK residents (and overwhelmingly citizens). This makes the *Schrems* statement a live issue. There are safeguards in place, in each case a warrant must be issued by the Secretary of State and must be approved by Judicial Commissioners. It is not therefore 'retention on a generalised basis' of communications and communications data but rather some form of targeted system. At least that's what the UK Government would say. However when we also know that GCHQ were using as few as 18 periodically renewed RIPA section 8(4) warrants to authorize TEMPORA as well as their other programmes,[102] allowing them to tap into the transatlantic fibre optic cables, which reportedly allowed them to processes 40 billion items of data per day: then these safeguards seem more illusory than real. The questions therefore become (i) is this 'legislation permitting the public authorities to have access [to communications and data] on a generalised basis' and (ii) will the additional safeguards of the Investigatory Powers Act, such as the introduction of Judicial Commissioners, protect the UK Government?

Conclusions

The evidence is clearly beginning to mount against the assumption that the UK will be able 'to secure the unhindered flow of data between the UK and the EU post-Brexit' as Mr Hancock would like. Whether negotiated as part of the Article 50 settlement, or separately as an adequacy decision, there are clear issues the UK Government needs to overcome regarding both data retention and mass surveillance. When this is placed against a backdrop of a likely failure of the UK domestic settlement to recognize an Article 8 right to Data Protection (as opposed to the operationalization of that right through GDPR style legislation) things begin to look bleak.

98 <http://www.ipt-uk.com/> 1 August 2017.

99 Above n 66, [94].

100 The British Islands is a legal definition of collective landmasses found in Schedule 1 of the Interpretation Act 1978. It is "the United Kingdom, the Channel Islands and the Isle of Man".

101 A discussion of what qualifies as an "overseas-related communication", or in the language of the Regulation of Investigatory Powers Act 2000, an external communication, may be found at *Liberty & Ors v GCHQ & Ors* [2014] UKIPTrib 13_77-H. <http://www.ipt-uk.com/docs/IPT_13_168-173_H.pdf> 1 August 2017.

102 Intelligence and Security Committee of Parliament, *Privacy and Security: A Modern and Transparent Legal Framework*, HC 1075, 12 March 2015, fn 83.

When one examines the *Schrems* decision some other issues emerge. The first is that even should an adequacy decision be issued, then as Max Schrems did himself, EU27 citizens concerned about the UK's state surveillance and data retention programme may challenge the transfer of their data to the UK via any EU27 supervisory authority.[103] Secondly, the duties of the Commission do not end with an adequacy decision. As the Court stated in *Schrems* 'in the light of the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted a decision pursuant to Article 25(6) of Directive 95/46, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard'.[104] Further 'as the Advocate General has stated in points 134 and 135 of his Opinion, when the validity of a Commission decision adopted pursuant to Article 25(6) of Directive 95/46 is examined, account must also be taken of the circumstances that have arisen after that decision's adoption'.[105]

Perhaps of most concern for the UK Government going forward is that such a review must be strict.[106] The possible impact of this is that even if the UK has some form of adequacy decision, whether negotiated as part of the Article 50 settlement, or as a separate Article 45 GDPR ruling, on 29 March 2019 an immediate challenge from a civil society group or individual along the lines of *Schrems* or *Digital Rights Ireland v Commission*[107] is quite likely given the UK's extensive framework of data retention and surveillance legislation, some of which treats EU27 residents (and thereby mostly citizens), differently to residents of the British Islands. It is not impossible that as a result of such a challenge, or even just in the fullness of time as details of how GCHQ and SIS/The Security Service operate under the Investigatory Powers Bill framework,[108] a review of any adequacy decision may be reversed applying the strict *Schrems* criteria.

It is clear that the realpolitik of Brexit is that a continued free flow of data between the EU27 and the UK is in the interests of all parties due to the extensive nature of the digital single market, GCHQ's vital role in SIGINT provision to Europe as a whole and London's continued, though perhaps diminished, role as the world's leading financial centre.[109] This will in all likelihood lead to some form of compromise position being reached before 29 March 2019 that will deliver to the UK the settlement they seek. However, this article suggests that it is folly to assume that the UK's legal framework guarantees this settlement merely by the implementation of the GDPR through domestic legislation. Further, although the position on 29 March 2019 may be that agreement on data transfers has been reached, we cannot assume that position would remain in effect indefinitely given the responsibility of the Commission to 'to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified'.[110]

doi:10.1093/idpl/ipx015
Advance Access Publication 25 August 2017

103 Above n 66, [40–41].

104 Ibid [76].

105 Ibid [77].

106 Ibid [78].

107 Case T-670/16, OJ 2016 C 410/26.

108 On which see Kieren McCarthy, 'Leaked: The UK's secret blueprint with telcos for mass spying on internet, phones – and backdoors. Real-time full-blown snooping with breakable encryption', *The Register* (4 May 2017) <https://www.theregister.co.uk/2017/05/04/uk_bulk_surveillance_powers_draft>.

109 On which see Karen McCullagh, 'Brexit: Potential Trade and Data Implications for Digital and "fintech" Industries' (2017) 7(1) IDPL 3.

110 *Maximillian Schrems v Data Protection Commissioner*, above n 66 at [64].

Appendix 3:

Report of Department for Exiting the European Union:

Legislating for the United Kingdom's withdrawal from the European Union

Department
for Exiting the
European Union

Legislating for the United Kingdom's withdrawal from the European Union

Cm 9446

Legislating for the United Kingdom's withdrawal from the European Union

Presented to Parliament
by the Secretary of State for Exiting the European Union
by Command of Her Majesty

March 2017

Cm 9446

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at repeal-bill@dexeu.gov.uk or Department for Exiting the European Union, 9 Downing Street, London SW1A 2AS

Print ISBN 9781474140058

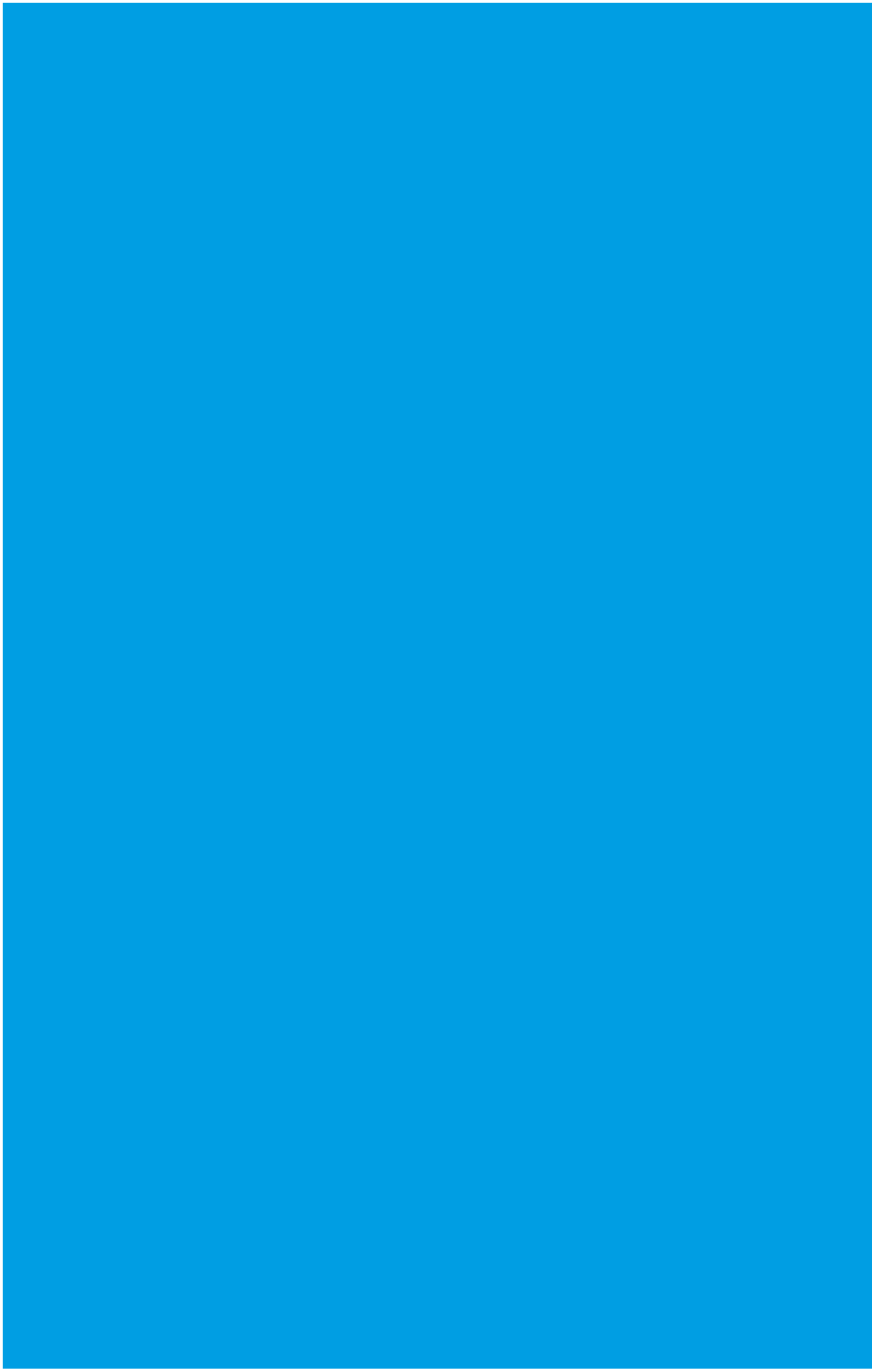
Web ISBN 9781474140065

ID 17011701 03/17 59227

Printed on paper containing 75% recycled fibre content minimum.

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office.

Contents



Foreword from the Prime Minister

The Government's first objective as we negotiate a new deep and special partnership with the European Union is to provide business, the public sector, and everybody in our country with as much certainty as possible as we move through the process.

This clarity will help people to plan effectively, recruit appropriately and invest as necessary while the negotiations continue and the new partnership we will enjoy with the European Union is being formed.

We have already been able to provide some clarity and reassurance in certain sectors. For example, last year the Government acted quickly to give certainty about farm payments and university funding. And we have also pledged to put the final deal that is agreed between the UK and the EU to a vote in both Houses of Parliament before it comes into force.

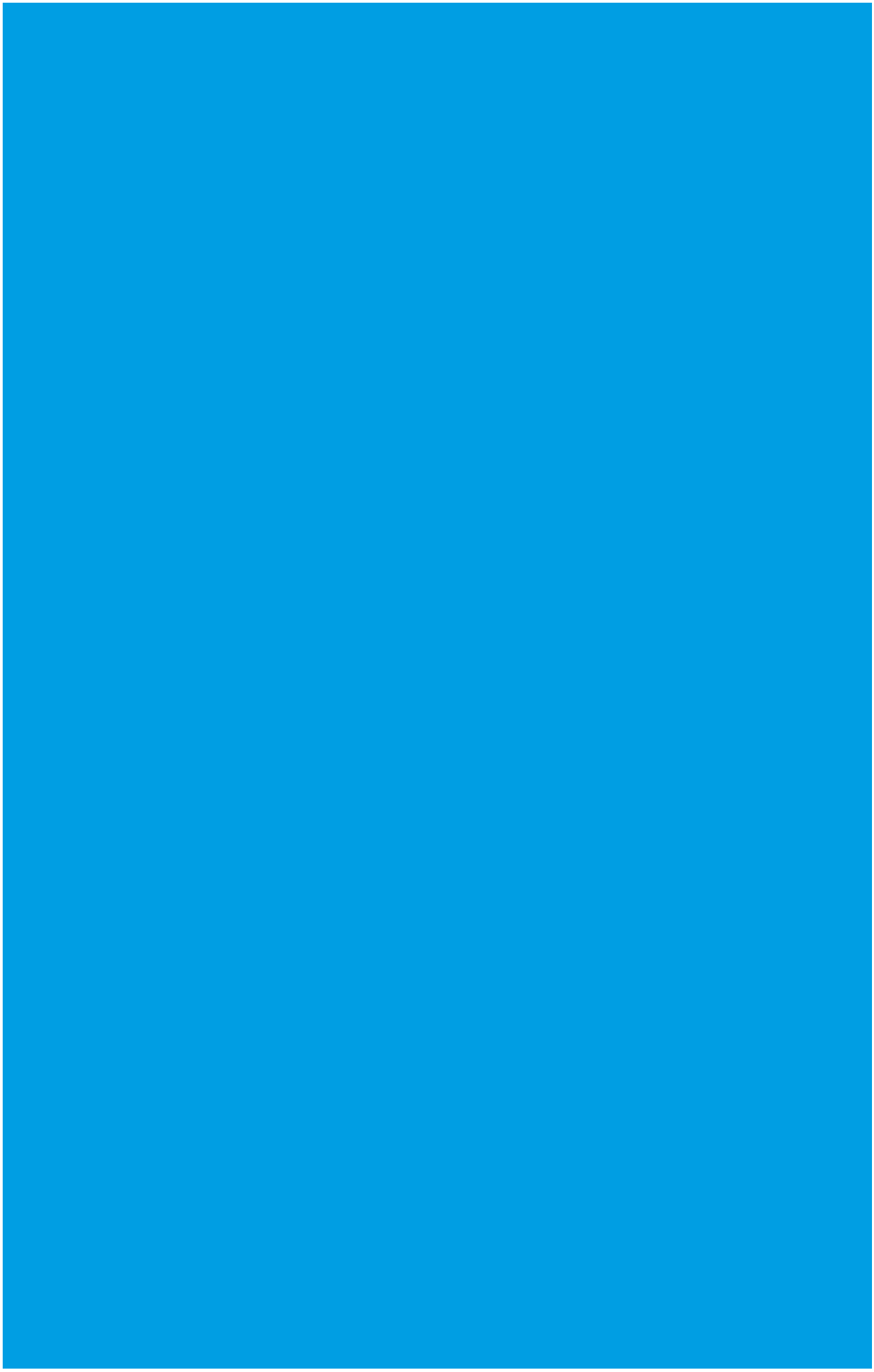
Our decision to convert the 'acquis' – the body of European legislation – into UK law at the moment we repeal the European Communities Act is an essential part of this plan.

This approach will provide maximum certainty as we leave the EU. The same rules and laws will apply on the day after exit as on the day before. It will then be for democratically elected representatives in the UK to decide on any changes to that law, after full scrutiny and proper debate.

This White Paper explains how we will legislate for this approach by introducing a Great Repeal Bill at the start of the next parliamentary session. This Bill will, wherever practical and appropriate, convert EU law into UK law from the day we leave so that we can make the right decisions in the national interest at a time that we choose.

The Great Repeal Bill is an important part of our plan to deliver a smooth and orderly Brexit that commands the confidence of all. The task ahead may be significant, but I am confident we can make it a success. This White Paper is an essential step along the way.

Rt Hon Theresa May MP
Prime Minister



Foreword from the Secretary of State for Exiting the European Union

On 23 June 2016 the United Kingdom made the historic decision to leave the European Union. In implementing that decision, we will build a great, global trading nation that is respected around the world and is strong, confident and united at home.

At the heart of that historic decision was sovereignty. A strong, independent country needs control of its own laws. That, more than anything else, was what drove the referendum result: a desire to take back control. That process starts now.

To achieve this, the Great Repeal Bill will repeal the European Communities Act 1972 on the day we leave the EU. The UK Parliament will unquestionably be sovereign again. Our courts will be the ultimate arbiters of our laws. In achieving this, we will be delivering on the outcome of the referendum.

But taking back control does not require us to change everything overnight – and we will not do so. Rather, we will provide for a smooth and orderly exit. The Great Repeal Bill will convert EU law as it applies in the UK into domestic law on the day we leave – so that wherever practical and sensible, the same laws and rules will apply immediately before and immediately after our departure. It is not a vehicle for policy changes – but it will give the Government the necessary power to correct or remove the laws that would otherwise not function properly once we have left the EU.

This substantial task of delivering a functioning statute book must be completed before we leave the EU – but the need to act at speed cannot be at the expense of ensuring the appropriate levels of parliamentary scrutiny.

As we leave the EU, we have an opportunity to ensure that returning powers sit closer to the people of the United Kingdom than ever before. In some areas where the existence of common frameworks at EU level has also provided common UK frameworks, it will be important to ensure that this stability and certainty are not compromised.

Examples of where common UK frameworks may be required include where they are necessary to protect the freedom of business to operate across the UK single market and to enable the UK to strike free trade deals.

Decisions will be required about whether a common framework is needed and, if it is, how it might be established. We will work closely with the devolved administrations to deliver an approach that works for the whole of the United Kingdom. But what is clear is that the outcome of this process will be a significant increase in the decision-making power of each devolved administration. As we bring powers back from Brussels, we will put them into the hands of democratically elected representatives in the United Kingdom.

I hope that people across the country will welcome the Bill's pragmatic but principled approach to maximising certainty, providing clarity and allowing for parliamentary scrutiny as we leave the EU.

Rt Hon David Davis MP
Secretary of State for Exiting the European Union

Chapter 1: Delivering the referendum result

1.1 On 1 January 1973 the United Kingdom joined the European Economic Community, which has since evolved to become today's European Union (EU). A condition of EU membership is that community law, which is now EU law, be given effect in domestic law. The European Communities Act 1972 (ECA) is the principal piece of legislation that gives effect to EU law in the UK and the legislation which makes EU law supreme over UK law.

1.2 After joining the European Economic Community, the UK adopted a number of subsequent treaties which were designed to establish greater political and economic integration between member states. In 1987, the Single European Act set a date for completion of the single market by the end of 1992, providing for the free movement of goods, persons, services and capital. In 1993, the Maastricht Treaty established the EU and created its three pillar structure, with the European Economic Community being the first pillar, the common foreign and security policy the second pillar and cooperation in justice and home affairs the third pillar.

1.3 Further changes were made by the Treaty of Amsterdam (1999) and the Treaty of Nice (2003). Following the expansion of the EU to include its current 28 member states, the Lisbon Treaty in 2009 renamed and amended the original treaties and collapsed the three pillar system into a single European Union.

1.4 Although the UK adopted the above EU treaties, the UK negotiated significant caveats to certain areas of EU membership. For example, during the Maastricht process the UK negotiated opt-outs, which exempted the country from Economic and Monetary Union and therefore the adoption of the Euro. The UK also secured a special status under the Treaty of Amsterdam, which safeguarded the UK's decision not to adopt the borders elements of the Schengen Agreement and certain other justice and home affairs matters, while the Lisbon Treaty saw the UK negotiate an opt-in process for individual police and criminal justice cooperation measures.

1.5 On 23 January 2013 the then Prime Minister announced his intention to negotiate a new settlement on the terms of the UK's membership of the EU, followed by a pledge to subsequently hold an in-out referendum on the UK's membership of the EU.

1.6 On 17 December 2015 the European Union Referendum Act 2015 – backed by an overwhelming majority of MPs – received Royal Assent. The Act made provision for holding a referendum in the United Kingdom and Gibraltar on whether the UK should remain a member of the EU. The Government committed to honouring the result. The referendum was then held on 23 June 2016.

1.7 **The result – by 52% to 48% – was a clear instruction from the people of the United Kingdom to leave the EU.**

1.8 The Prime Minister was clear that there would be no unnecessary delays in invoking Article 50 of the Treaty on European Union, which began our formal negotiations to leave the EU. The European Union (Notification of Withdrawal) Act 2017 was passed into law on 16 March and gave the Prime Minister the legal authority to notify under Article 50. This notification was then given on 29 March.

1.9 Article 50 is the only legal route by which we can leave the EU. It sets out that the UK has two years to negotiate a withdrawal agreement with the EU, after which our membership of the EU will end unless an extension is agreed with the European Council.

1.10 The UK remains a full member of the EU and all the rights and obligations of EU membership remain in force until exit. The Government will continue to negotiate, implement and apply EU law during this period.

1.11 The Article 50 process gives effect to the UK's withdrawal as a matter of EU law. However, new primary legislation is needed to ensure that the domestic statute book reflects the UK's withdrawal from the EU, and to ensure an orderly transition from EU membership. **We need to be in a position to repeal the ECA on the day we leave the EU.**

1.12 In order to achieve a stable and smooth transition, the Government's overall approach is to convert the body of existing EU law into domestic law, after which Parliament (and, where appropriate, the devolved legislatures) will be able to decide which elements of that law to keep, amend or repeal once we have left the EU. **This ensures that, as a general rule, the same rules and laws will apply after we leave the EU as they did before.**

1.13 **If the Great Repeal Bill did not convert existing EU law into domestic law at the same time as repealing the ECA**, the UK's statute book would contain significant gaps once we left the EU. There are a large number of EU regulations and many other EU-derived laws which form part of our law which, if we were to repeal the ECA without making further provision, would no longer apply, creating large holes in our statute book.

1.14 Simply incorporating EU law into UK law is not enough, however. A significant amount of EU-derived law, even when converted into domestic law, will not achieve its desired legal effect in the UK once we have left the EU. For example, legislation may refer to the involvement of an EU institution or be predicated on UK membership of, or access to, an EU regime or system. Once we have left the EU, this legislation will no longer work. Government must act to ensure that the domestic statute book continues to function once we have left the EU.

1.15 That said, it is neither possible nor desirable for all of the changes that will be needed to domestic law to be made in the Great Repeal Bill itself. This is for a number of reasons, including that the nature and timing of many of the necessary changes do not lend themselves to inclusion in primary legislation. Also, some of the changes will be to devolved law and would be better made by devolved institutions. As such, the Great Repeal Bill will create a power to correct the statute book where necessary, to rectify problems occurring as a consequence of leaving the EU. This will be done by secondary legislation.

1.16 It is also important to recognise that the timing of the Great Repeal Bill and associated secondary legislation will run in parallel to the negotiation process under Article 50. This means undertaking the legislative process necessary to correct the statute book while

the negotiations are underway. There is much that can be taken forward during those negotiations, but some legislation will necessarily need to await their conclusion. The approach outlined in this White Paper is designed to give businesses, workers, investors and consumers the maximum possible certainty as we leave the EU: but it also needs to provide the flexibility necessary to respond to all eventualities of the negotiation process.

1.17 The House of Lords Constitution Committee published a report on 7 March 2017 that stated "further amendments to domesticated EU law (i.e. the body of EU law that will be made part of UK law after Brexit) will be needed in order to implement the final withdrawal agreement. While the Government will need to get the separate approval of Parliament to this agreement, it may well choose to use powers granted under the 'Great Repeal Bill' to prepare some of the necessary changes to domesticated EU law to take effect on Brexit-day".[1]

1.18 We agree with the Committee that the Great Repeal Bill should also provide the Government with a further limited power to implement the contents of any withdrawal agreement reached with the EU into our domestic law without delay, where it is necessary to do so in order that we are ready to begin a new partnership from exit.

1.19 This is a separate process from that by which the Government will bring forward a motion on the final agreement to be voted on by both Houses of Parliament before it is concluded. Any new treaty that we agree with the EU will also be subject to the provisions of the Constitutional Reform and Governance Act 2010 before ratification.

1.20 The Government is confident that the UK can reach a positive agreement about our future relationship with the EU in the time available under Article 50. However, we have also been clear that no deal for the UK is better than a bad deal for the UK. The Great Repeal Bill would also support the scenario where the UK left the EU without a deal in place, by facilitating the creation of a complete and functioning statute book no longer reliant on EU membership.

1.21 The Great Repeal Bill will not aim to make major changes to policy or establish new legal frameworks in the UK beyond those which are necessary to ensure the law continues to function properly from day one. Therefore, the Government will also introduce a number of further bills during the course of the next two years to ensure we are prepared for our withdrawal – and that Parliament has the fullest possible opportunity to scrutinise this legislation.

1.22 For example, we will introduce a customs bill to establish a framework to implement a UK customs regime. The requirement for a UK customs regime cannot be met merely by incorporating EU law – and would benefit from the intensive parliamentary scrutiny given to primary legislation. Similarly, we will introduce an immigration bill so nothing will change for any EU citizen, whether already resident in the UK or moving from the EU, without Parliament's approval. This is in line with our overall approach to the Great Repeal Bill – not to make major policy changes through or under the Bill, but to allow Parliament an opportunity to debate our future approach and give effect to that through separate bills. New legislation will be required to implement new policies or institutional arrangements that go beyond replicating current EU arrangements in UK law.

[1] 'The 'Great Repeal Bill' and delegated powers', Lords Select Committee on the Constitution, 9th Report of Session 2016-17, 7 March 2017, page 13, https://www.publications.parliament.uk/pa/ld201617/ldselect/ldconst/123/123.pdf

Summary of main provisions

1.23 In summary, therefore, the Great Repeal Bill will put the UK back in control of its laws; maximise certainty for businesses, workers, investors and consumers across the whole of the UK as we leave the EU; and ensure accountability for the powers contained in the Bill.

1.24 To achieve this, the Great Repeal Bill will do three main things:

a. First, it will **repeal the ECA** and return power to UK institutions.

b. Second, subject to the detail of the proposals set out in this White Paper, the Bill will **convert EU law** as it stands at the moment of exit into UK law before we leave the EU. This allows businesses to continue operating knowing the rules have not changed significantly overnight, and provides fairness to individuals, whose rights and obligations will not be subject to sudden change. It also ensures that it will be up to the UK Parliament (and, where appropriate, the devolved legislatures) to amend, repeal or improve any piece of EU law (once it has been brought into UK law) at the appropriate time once we have left the EU.

c. Finally, the Bill will **create powers to make secondary legislation.** This will enable corrections to be made to the laws that would otherwise no longer operate appropriately once we have left the EU, so that our legal system continues to function correctly outside the EU, and will also enable domestic law once we have left the EU to reflect the content of any withdrawal agreement under Article 50.

1.25 Chapter 2 sets out the Government's approach to the repeal of the ECA and the conversion of EU law into UK law. Chapter 3 considers the powers in the Bill to make secondary legislation. Chapter 4 looks at the interaction between the Bill's provisions and the devolution settlements, while Chapter 5 looks at the impact on the Crown Dependencies and Overseas Territories.

1.26 The Government welcomes feedback on this White Paper. Comments can be sent to repeal-bill@dexeu.gov.uk.

Chapter 2: Our approach to the Great Repeal Bill

Repeal of the European Communities Act 1972

2.1 The ECA gives effect in UK law to the EU treaties. It incorporates EU law into the UK domestic legal order and provides for the supremacy of EU law. It also requires UK courts to follow the rulings of the Court of Justice of the European Union (CJEU).

2.2 Some EU law applies directly without the need for specific domestic implementing legislation, while other parts of EU law need to be implemented in the UK through domestic legislation. As explained later in this White Paper, domestic legislation other than the ECA also gives effect to some of the UK's obligations under EU law.

2.3 As a first step, it is important to repeal the ECA to ensure there is maximum clarity as to the law that applies in the UK, and to reflect the fact that following the UK's exit from the EU it will be UK law, not EU law, that is supreme. The Bill will repeal the ECA on the day we leave the EU.

Converting EU law into UK law

2.4 Simply repealing the ECA would lead to a confused and incomplete legal system. This is because, as described above, some types of EU law (such as EU regulations) are directly applicable in the UK's legal system. This means they have effect here without the need to pass specific UK implementing legislation. They will therefore cease to have effect in the UK once we have left the EU and repealed the ECA, leaving large holes in the statute book. To avoid this, **the Bill will convert directly-applicable EU laws into UK law**.

2.5 By contrast, other types of EU law (such as EU directives) have to be given effect in the UK through national laws. This has frequently been done using section 2(2) of the ECA, which provides ministers, including in the devolved administrations, with powers to make secondary legislation to implement EU obligations. Once the ECA has been repealed, all of the secondary legislation made under it would fall away. As this would also leave a significant gap in the statute book, **the Bill will also preserve the laws we have made in the UK to implement our EU obligations**.

What does the Great Repeal Bill convert into UK law?

The Bill will ensure that, wherever possible, the same rules and laws apply on the day after we leave the EU as before.

This means that:

- the Bill will convert directly-applicable EU law (EU regulations) into UK law (paragraph 2.4);
- it will preserve all the laws we have made in the UK to implement our EU obligations (paragraph 2.5);
- the rights in the EU treaties that can be relied on directly in court by an individual will continue to be available in UK law (paragraph 2.11); and
- the Bill will provide that historic CJEU case law be given the same binding, or precedent, status in our courts as decisions of our own Supreme Court (paragraphs 2.12 to 2.17).

2.6 There is no single figure for how much EU law already forms part of UK law. According to EUR-Lex, the EU's legal database, there are currently over 12,000 EU regulations in force (this includes amending regulations as well as delegated and implementing regulations).[2] In terms of domestic legislation which implements EU law such as directives, research from the House of Commons Library indicates that there have been around 7,900 statutory instruments which have implemented EU legislation. This figure does not include statutory instruments made by the devolved administrations which will also observe and implement EU obligations in areas within their competence.[3] In addition, research from the House of Commons Library indicates that out of 1,302 UK Acts between 1980 and 2009 (excluding those later repealed), 186 Acts (or 14.3%) incorporated a degree of EU influence.[4]

2.7 Our approach of converting EU law into domestic law maximises certainty and stability while ensuring Parliament is sovereign. For the purposes of this paper we are calling this body of law 'EU-derived law'. The Government considers that, unless and until domestic law is changed by legislators in the UK, legal rights and obligations in the UK should where possible be the same after we have left the EU as they were immediately before we left.

2.8 EU regulations will not be 'copied out' into UK law regulation by regulation. Instead the Bill will make clear that EU regulations – as they applied in the UK the moment before we left the EU – will be converted into domestic law by the Bill and will continue to apply until legislators in the UK decide otherwise.

[2] EUR-Lex search run on 28 March 2017: http://eur-lex.europa.eu/search.html?qid=1490700962298&VV=true&DB_TYPE_OF_ACT=allRegulation&DTC=false&DTS_DOM=EU_LAW&typeOfActStatus=ALL_REGULATION&type=advanced&lang=en&SUBDOM_INIT=LEGISLATION&DTS_SUBDOM=LEGISLATION

[3] 'Legislating for Brexit: Statutory Instruments implementing EU law', House of Commons Library Research Paper 7867, 16 January 2017, page 6, http://researchbriefings.files.parliament.uk/documents/CBP-7867/CBP-7867.pdf

[4] 'How much legislation comes from Europe?', House of Commons Library Research Paper 10/62, 13 October 2010, page 19, http://researchbriefings.files.parliament.uk/documents/RP10-62/RP10-62.pdf

The EU treaties

2.9 The treaties are the primary source of EU law. A substantial proportion of the treaties sets out rules for the functioning of the EU, its institutions and its areas of competence. While much of the content of the treaties will become irrelevant once the UK leaves the EU, the treaties (as they exist at the moment we leave the EU) may assist in the interpretation of the EU laws we preserve in UK law.

2.10 For example, in interpreting an EU measure it may be relevant to look at its aim and content, as revealed by its legal basis as found in the treaties. In interpreting workers' annual leave entitlement, the legal basis of the Working Time Directive was found to be relevant.[5] The court found that member states could not adopt national rules under which workers' rights to paid annual leave depended on their having completed a minimum period of employment with the same employer. Had the court not looked to original treaty provisions giving rise to the Working Time Directive, it may have given the directive an alternative meaning. Once we have left the EU, our courts will continue to be able to look to the treaty provisions in interpreting EU laws that are preserved.

2.11 Equally, there are rights in the EU treaties that can be relied on directly in court by an individual, and the Great Repeal Bill will incorporate those rights into UK law. The text box overleaf on workers' rights gives an illustration of why this is important in practice.

Case law of the Court of Justice of the European Union (CJEU)

2.12 The Government has been clear that in leaving the EU we will bring an end to the jurisdiction of the CJEU in the UK. Once we have left the EU, the UK Parliament (and, as appropriate, the devolved legislatures) will be free to pass its own legislation.

2.13 The Great Repeal Bill will not provide any role for the CJEU in the interpretation of that new law, and the Bill will not require the domestic courts to consider the CJEU's jurisprudence. In that way, the Bill allows the UK to take control of its own laws. We will, of course, continue to honour our international commitments and follow international law.

2.14 However, for as long as EU-derived law remains on the UK statute book, it is essential that there is a common understanding of what that law means. The Government believes that this is best achieved by providing for continuity in how that law is interpreted before and after exit day. To maximise certainty, therefore, the Bill will provide that any question as to the meaning of EU-derived law will be determined in the UK courts by reference to the CJEU's case law as it exists on the day we leave the EU. Everyone will have been operating on the basis that the law means what the CJEU has already determined it does, and any other starting point would be to change the law. Insofar as case law concerns an aspect of EU law that is not being converted into UK law, that element of the case law will not need to be applied by the UK courts.

2.15 For example, CJEU case law governs the calculation of holiday pay entitlements for UK workers: failure to carry across that case law would be to create uncertainty for workers and employers. Similarly, CJEU case law has over the past four decades clarified what is and is not subject to VAT, and failing to follow that case law in our own legal system would create new uncertainties about the application of VAT.

[5] Case C-173/99 *BECTU v Secretary of State Trade and Industry* [2001] ECR I-4881, http://curia.europa.eu/juris/liste.jsf?language=en&num=C-173/99

2.16 This approach maximises legal certainty at the point of departure, but the intention is not to fossilise the past decisions of the CJEU forever. As such, we propose that the Bill will provide that historic CJEU case law be given the same binding, or precedent, status in our courts as decisions of our own Supreme Court. It is very rare for the Supreme Court to depart from one of its own decisions or that of its predecessor, the House of Lords. The circumstances in which it will, exceptionally, do so, derive from a Practice Statement made by the House of Lords in 1966, and adopted by the Supreme Court in 2010. That Statement set out, among other things, that while treating its former decisions as normally binding, it will depart from its previous decisions "when it appears right to do so".

2.17 We would expect the Supreme Court to take a similar, sparing approach to departing from CJEU case law. We are also examining whether it might be desirable for any additional steps to be taken to give further clarity about the circumstances in which such a departure might occur. Parliament will be free to change the law, and therefore overturn case law, where it decides it is right to do so.

Example 1: Workers' rights and equalities

The Great Repeal Bill will convert EU law into domestic law. This means that the workers' rights that are enjoyed under EU law will continue to be available in UK law after we have left the EU. Where protections are provided by the EU treaties as a final 'backstop' – such as the right to rely on Article 157 of TFEU (equal pay) directly in court – they will also be preserved.

Protections are further strengthened by the Great Repeal Bill's incorporation of CJEU case law (see paragraphs 2.12 to 2.17), which means that where workers' rights have been extended by CJEU judgments, those rights will continue to be protected in the UK once we have left the EU. In a number of areas, UK employment law already goes further than the minimum standards set out in EU legislation, and this Government will continue to protect and enhance the rights people have at work.

Furthermore, all the protections covered in the Equality Act 2006, the Equality Act 2010 and equivalent legislation in Northern Ireland will continue to apply once the UK has left the EU. This approach will give certainty to service providers and users, as well as employees and employers, creating stability in which the UK can grow and thrive.

Example 2: Environmental protection

The Government is committed to ensuring that we become the first generation to leave the environment in a better state than we found it.

The UK's current legislative framework at national, EU and international level has delivered tangible environmental benefits, such as cleaner rivers and reductions in emissions of sulphur dioxide and ozone depleting substances emissions. Many existing environmental laws also enshrine standards that affect the trade in products and substances across different markets, within the EU as well as internationally.

The Great Repeal Bill will ensure that the whole body of existing EU environmental law continues to have effect in UK law. This will provide businesses and stakeholders with maximum certainty as we leave the EU. We will then have the opportunity, over time, to ensure our legislative framework is outcome driven and delivers on our overall commitment to improve the environment within a generation. The Government recognises the need to consult on future changes to the regulatory frameworks, including through parliamentary scrutiny.

Example 3: Consumer protection

UK consumer law predates EU competence in this area, and goes beyond EU minimum requirements in a number of respects. For example, the right for UK consumers to reject a faulty good within a 30-day period is a UK-level protection, and traders are limited to a single attempt to repair or replace a faulty product before having to offer a refund. In addition, the UK has legislated to make sure that consumers have clear rights when buying digital content.

Where consumer protections are set at the EU level and thus already part of UK law, the Great Repeal Bill will preserve the relevant EU law to ensure domestic law functions properly after exit. This stability will give businesses and consumers clarity and confidence in their rights and obligations, facilitating the day-to-day transactions that keep the UK economy strong. It will help ensure that UK consumers' rights continue to be robust after we have left the EU.

In addition, the Government intends to bring forward a Green Paper this spring which will closely examine markets which are not working fairly for consumers.

Supremacy of EU law

2.18 The UK Parliament remains sovereign, and parliamentary sovereignty is the foundation of the UK constitution. As a consequence of the ECA, passed by the UK Parliament, case law makes it clear that EU law has supremacy for as long as we are a member state. National laws must give way and be disapplied by domestic courts if they are found to be inconsistent with EU law.

2.19 Our proposed approach is that, where a conflict arises between EU-derived law and new primary legislation passed by Parliament after our exit from the EU, then newer legislation will take precedence over the EU-derived law we have preserved. In this way, **the Great Repeal Bill will end the general supremacy of EU law**.

2.20 If, after exit, a conflict arises between two pre-exit laws, one of which is an EU-derived law and the other not, then the EU-derived law will continue to take precedence over the other pre-exit law. Any other approach would change the law and create uncertainty as to its meaning. This approach will give coherence to the statute book, while putting Parliament back in control. Once the UK has left the EU, Parliament (and, where appropriate, the devolved legislatures) will be able to change these laws wherever it is considered desirable.

Charter of Fundamental Rights

2.21 One of the general principles of EU law is respect for fundamental rights, which includes many of the rights we refer to as human rights in the UK. In leaving the EU, the UK's leading role in protecting and advancing human rights will not change. The EU codifies fundamental rights in the Charter of Fundamental Rights, which has the same legal status as the EU treaties.

2.22 The Charter is only one element of the UK's human rights architecture. Many of the rights protected in the Charter are also found in other international instruments, notably the European Convention on Human Rights (ECHR), but also UN and other international treaties too. The ECHR is an instrument of the Council of Europe, not of the EU. The UK's withdrawal from the EU will not change the UK's participation in the ECHR and there are no plans to withdraw from the ECHR.

2.23 The Charter only applies to member states when acting within the scope of EU law, so its relevance is removed by our withdrawal from the EU. Some rights will naturally fall away as we leave the EU, such as the right to vote or stand as a candidate in European Parliament elections. It cannot be right that the Charter could be used to bring challenges against the Government, or for UK legislation after our withdrawal to be struck down on the basis of the Charter. On that basis the Charter will not be converted into UK law by the Great Repeal Bill.

2.24 However, the Charter was not designed to create any new rights or alter the circumstances in which individuals could rely on fundamental rights to challenge the actions of the EU institutions or member states in relation to EU law. Instead the Charter was intended to make the rights that already existed in EU law more visible by bringing them together in a single document.

2.25 The Government's intention is that the removal of the Charter from UK law will not affect the substantive rights that individuals already benefit from in the UK. Many of these underlying rights exist elsewhere in the body of EU law which we will be converting into UK law. Others already exist in UK law, or in international agreements to which the UK is a party. As EU law is converted into UK law by the Great Repeal Bill, it will continue to be interpreted by UK courts in a way that is consistent with those underlying rights. Insofar as cases have been decided by reference to those underlying rights, that case law will continue to be relevant. In addition, insofar as such cases refer to the Charter, that element will have to be read as referring only to the underlying rights, rather than to the Charter itself.

Chapter 3: Delegated powers in the Great Repeal Bill

The challenge

3.1 By repealing the ECA, we are removing parts of the legal framework under which the UK has operated for more than forty years. The previous chapter set out the Government's approach to ensure that this does not leave large holes on the statute book; namely, we will convert the corpus of EU law as it stands when we leave the EU into our domestic law. This action alone will not, though, be sufficient to provide a smooth and orderly exit.

3.2 A large amount of EU law currently applies in the UK. A proportion of this will continue to operate properly once we have left the EU simply by converting it into UK law. For example, large parts of employment law will continue to function properly once we have left the EU. But an even larger proportion of the converted law will not function effectively once we have left the EU unless we take action to correct it.

3.3 There is a variety of reasons why conversion alone may not be sufficient in particular cases. There will be gaps where some areas of converted law will be entirely unable to operate because we are no longer a member of the EU. There will also be cases where EU law will cease to operate as intended or will be redundant once we leave. In some cases EU law is based on reciprocal arrangements, with all member states treating certain situations in the same way. If such reciprocal arrangements are not secured as a part of our new relationship with the EU, it may not be in the national interest, or workable, to continue to operate those arrangements alone.

3.4 Similar issues will arise in legislation made by devolved ministers or enacted by devolved legislatures (discussed further in Chapter 4). The case studies below provide examples of the different types of legal corrections which would need to be made once we leave the EU, and how the power will enable the Government to address them.

Case study 1: references to "EU law"

Throughout the statute book, there are references which will no longer be accurate once we leave the EU, such as references to *"Member States other than the United Kingdom"*, to *"EU law"* or to providing for the UK's *"EU obligations"*. Such references will need to be repealed or amended to ensure we have a comprehensive statute book post-exit.

In this instance, the power to correct would allow the Government to amend converted law to reflect our new position. For example, section 171 of the Enterprise Act 2002 requires the Competition and Markets Authority to publish advice and information about the operation of certain provisions of that Act which must include information about the effect of EU law on those provisions. That reference and the definition of *"EU law"* in section 171 will need amending or repealing to reflect the fact that EU law will no longer apply once the UK exits the EU.

Case study 2: involvement of an EU institution

There will be law which will, upon leaving the EU, no longer work at all and which will need to be corrected to continue to work. An example of this would be the Offshore Petroleum Activities (Conservation of Habitats) Regulations 2001.[6] These domestic regulations contain a requirement to obtain an opinion from the European Commission on particular projects relating to offshore oil and gas activities. Once we leave the EU, the Commission will no longer provide such opinions to the UK (and we would not seek them). However, this requirement in the existing regulations would prevent certain projects from taking place unless we correct it.

In this instance the power to correct the law would allow the Government to amend our domestic legislation to either replace the reference to the Commission with a UK body or remove this requirement completely.

[6] See Regulation 6(2)(b) of the Offshore Petroleum Activities (Conservation of Habitats) Regulations 2001 (S.I. 2001/1754), http://www.legislation.gov.uk/uksi/2001/1754/contents/made

Case study 3: information sharing with EU institutions

Once we leave the EU, there will be areas of law where policy no longer operates as intended. This is the case where legislation would continue to work legally and can be complied with, but where the policy outcome delivered by that legislation might cease to make sense.

For example, this will happen where preserved legislation will continue to require the UK to send information to EU institutions (or offices, bodies or agencies) or EU member states. The UK would still be able to comply with such requirements in legislation to send information where there would be no legal barrier to doing so (i.e. the law would still function). However, where the UK had not explicitly agreed during exit negotiations to continue to provide such information to the EU, there may well be reasons why the UK would no longer wish to send such information after we exit the EU, and where it would make sense to amend the legislation to avoid previously reciprocal arrangements becoming one-sided.

An example of this would be the requirement for the UK to provide the European Commission with data relating to inland waterways transport as set out in Regulation 1365/2006.[7] In this case where the law no longer functions as intended, the power would allow the Government to amend or repeal these preserved regulations to reflect that such an arrangement only exists if it is in the UK's interest.

Of course in some cases we may want to exchange data with the EU, for example, for security matters.

3.5 Government departments have been analysing the UK statute book and directly-applicable EU law in their areas of responsibility to enable an assessment of the scale of the changes needed. It is clear that a very significant proportion of EU-derived law for which Government departments are responsible contains some provisions that will not function appropriately if EU law is simply preserved.[8]

3.6 Similar issues will also exist in legislation that is the responsibility of the devolved legislatures or ministers, such as that made under the ECA. UK Government legal advisers have been engaging with their colleagues in the devolved administrations to help determine the scale of the changes needed. The Bill will therefore give the devolved ministers a power to amend devolved legislation to correct law that will no longer operate appropriately, in line with the power held by UK ministers.

The proposed solution: delegated powers

3.7 To overcome the challenge set out above, **the Great Repeal Bill will provide a power to correct the statute book, where necessary, to rectify problems occurring as a consequence of leaving the EU**. This will be done using secondary legislation, and will help make sure we have put in place the necessary corrections before the day we exit the EU.

[7] Regulation (EC) No 1365/2006 of the European Parliament and of the Council of 6 September 2006 on statistics of goods transport by inland waterways and repealing Council Directive 80/1119/EEC, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006R1365

[8] This is based on a first trawl of the UK statute book by Government departments

3.8 Primary legislation can provide a framework within which Government can propose secondary legislation for parliamentary approval. Ultimately, the power to make secondary legislation is granted by Parliament and each use of these powers is subject to Parliament's control.

3.9 It is important that where Government policies are delivered by secondary legislation, the case for that decision is justified. There is a variety of reasons why, in a particular case, secondary legislation is needed and the relevant content is not suited for inclusion in primary legislation. In the context of the Great Repeal Bill, relevant reasons for using secondary legislation include:

a. matters which cannot be known or may be liable to change at the point when the primary legislation is being passed because the Government needs to allow for progress of negotiations;

b. adjustments to policy that are directly consequential on our exiting the EU; and

c. to provide a level of detail not thought appropriate for primary legislation.

3.10 The extent of secondary legislation that may be needed under the Bill has recently been the subject of a report by the House of Lords Select Committee on the Constitution. The Committee put this as being a difference between "the more mechanical act of converting EU law into UK law, and the discretionary process of amending EU law to implement new policies in areas that previously lay within the EU's competence", which the Committee thought should be done through primary legislation.[9] While there is inevitably a degree of discretion in how to undertake even the first of these categories, the Government agrees that the purpose of the Great Repeal Bill and the secondary legislation is to convert EU law into UK law.

3.11 In this particular instance, without powers to resolve the types of issues set out earlier in this chapter through secondary legislation, we would require a prohibitively large amount of primary legislation to correct these problems.

3.12 Clearly it is not possible to predict at this stage how every law is to be corrected, as in some areas of policy the solution may depend on the outcome of negotiations. The powers in the Bill will ensure that, whatever the outcome of those negotiations, the statute book can continue to function, and that decisions can be taken in the national interest and reflect the contents of the Withdrawal Agreement.

3.13 The Committee also reflected that "it is unrealistic to assume that Parliament will be able tightly to limit the delegated powers granted under the Bill", because to do so would unduly constrain the Government's ability to adapt converted EU law to fit the UK's post-exit circumstances. It also recognised that the circumstances "will almost certainly necessitate the granting of relatively wide delegated powers to amend existing EU law and to legislate for new arrangements following Brexit".[10]

[9] 'The 'Great Repeal Bill' and delegated powers', Lords Select Committee on the Constitution, 9th Report of Session 2016-17, 7 March 2017, page 10 https://www.publications.parliament.uk/pa/ld201617/ldselect/ldconst/123/123.pdf

[10] 'The 'Great Repeal Bill' and delegated powers', Lords Select Committee on the Constitution, 9th Report of Session 2016-17, 7 March 2017, pages 16 and 17 https://www.publications.parliament.uk/pa/ld201617/ldselect/ldconst/123/123.pdf

What is secondary legislation and how is it used?

Secondary legislation should not be misinterpreted as 'executive orders' issued by the Government. Rather, the use of secondary legislation is a legislative process of long standing. Statutory instruments, as a category of legislation, are governed by the Statutory Instruments Act 1946. Existing parliamentary procedures allow for Parliament to scrutinise as many or as few statutory instruments as it sees fit. Parliament can, and regularly does, both debate and vote on secondary legislation. Indeed, a large amount of EU law is implemented under the ECA through secondary legislation; although EU regulations are not approved by the UK Parliament at all, as they are directly applicable in UK law. The Government proposes that the Great Repeal Bill will use existing types of statutory instrument procedure.

3.14 The Committee also rightly identified the need to ensure that there are clear limitations on the use of secondary legislation in the context of EU exit – in terms of the purposes for which it can be used, the processes that have to be followed in using it, and the length of time for which powers are available.

3.15 The remainder of this chapter sets out some of the expected constraints on the use of this delegated power. The Government will give more specific assurances to Parliament about the limits of this power as it makes the case for it being granted. However, this will need to be balanced against ensuring the power is broad enough to make all of the necessary amendments to the statute book within the timeframe determined by the EU withdrawal process.

The scope of, and constraints on, the delegated powers

3.16 It is crucial that the Government is equipped to make all the necessary corrections to the statute book before we leave the EU to ensure a smooth and orderly withdrawal. To achieve this, the power to enable this correction will need to allow changes to be made to the full body of EU-derived law. This will necessarily include existing primary as well as secondary legislation which implements our EU obligations, as well as directly applicable EU law which will be converted into domestic law once we leave. It will also include the power to transfer to UK bodies or ministers powers that are contained in EU-derived law and which are currently exercised by EU bodies. This does mean that the power will be wide in terms of the legislation to which it can be used to make changes.

3.17 Therefore, it is important that the purposes for which the power can be used are limited. Crucially, we will ensure that the power will not be available where Government wishes to make a policy change which is not designed to deal with deficiencies in preserved EU-derived law arising out of our exit from the EU. Additionally, we will consider the constraints placed on the delegated power in section 2 of the ECA to assess whether similar constraints may be suitable for the new power, for example preventing the power from being used to make retrospective provision or impose taxation.

3.18 The scope of the power and the volume of primary legislation are intrinsically linked: if the power is too narrow, many more of the changes to legislation which are needed to ensure policy and legislation operate smoothly post-exit would need to be made through separate primary legislation before we leave the EU.

Statutory Instrument procedure

3.19 Making sure domestic law works as we leave the EU will be a substantial challenge for both Government and Parliament in complexity and planning to deal with a number of scenarios. In the previous two Parliaments, an average of 1,338 (2005-10) and 1,071 (2010-15) statutory instruments were made per year.[11] A proportion of this secondary legislation, as it has been every year, was implementing EU law. We currently estimate that the necessary corrections to the law will require between 800 and 1,000 statutory instruments. This is in addition to those statutory instruments that will be necessary for purposes other than leaving the EU. Ultimately though, it is not possible to be definitive at the outset about the volume of legislation that will be needed, as it will be consequent on the outcome of negotiations with the EU and other factors.

3.20 Parliament will need to be satisfied that the procedures in the Bill for making and approving the secondary legislation are appropriate. Given the scale of the changes that will be necessary and the finite amount of time available to make them, there is a balance that will have to be struck between the importance of scrutiny and the speed of this process.

3.21 The Government proposes using existing types of statutory instrument procedure.[12] These allow Parliament to see all statutory instruments, with different levels of scrutiny. The most commonly used procedures are the negative procedure (which does not require debate) and the affirmative procedure (which requires debate and approval by both Houses). Parliamentary committees scrutinise statutory instruments for technical and policy content. Under the negative procedure, members of either House can require a debate, and if necessary, require a vote.

3.22 The Bill will therefore provide for the negative and affirmative procedures to be used. The mechanistic nature of the conversion of EU law to UK law suggests that many statutory instruments will follow the negative procedure (for example, removing the requirement to send reports to the Commission on the UK's public procurement activity). The affirmative procedure may be appropriate for the more substantive changes.

3.23 **The Government is mindful of the need to ensure that the right balance is struck between the need for scrutiny and the need for speed. This White Paper is the beginning of a discussion between Government and Parliament as to the most pragmatic and effective approach to take in this area.**

Time limits

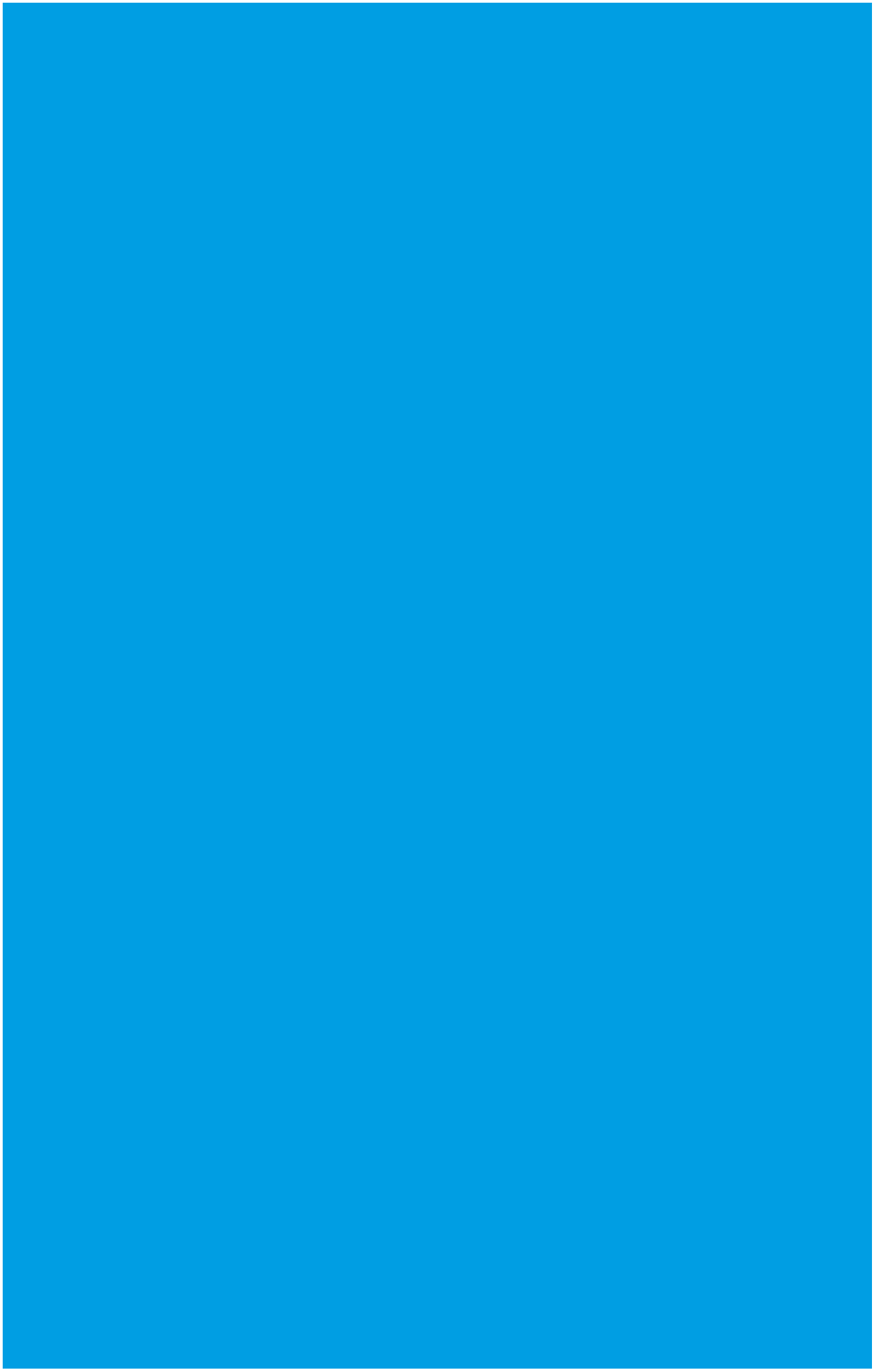
3.24 In most cases, the corrections made by the statutory instruments will need to be made before the UK leaves the EU, so that we have a functioning statute book on the day of the UK's withdrawal. The Government intends therefore that the power in the Great Repeal Bill will come into force as soon as the Bill gains Royal Assent, so that the process of correcting the statute book can begin.

[11] These averages are for Westminster statutory instruments subject to specific parliamentary procedure and scrutiny

[12] The various types of scrutiny procedure for statutory instruments are described in House of Commons Library note SN06509, available at 'Statutory Instruments', House of Commons Library Briefing Paper Number 06509, 15 December 2016. http://researchbriefings.files.parliament.uk/documents/SN06509/SN06509.pdf

3.25 Given that most of these corrections can and will need to be made before the UK leaves the EU, the powers proposed under the Bill do not need to exist in perpetuity. The Government will therefore ensure that the power is appropriately time-limited to enact the required changes.[13]

[13] The importance of time limiting delegated powers was raised by Baroness Fookes (Chair of the House of Lords Delegated Powers and Regulatory Reform Committee) in an evidence session held by the Lords Constitution Committee on 25 January 2017, as part of the Committee's inquiry on the Legislative Process: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/constitution-committee/legislative-process/oral/46201.htm, Q131



Chapter 4: Interaction with the devolution settlements

4.1 The United Kingdom's domestic constitutional arrangements have evolved since the UK joined the European Economic Community in 1973. The current devolution settlements were agreed after the UK became a member of what is now the EU and reflect that context. The devolved settlements were, therefore, premised on EU membership. This is why all three settlements set out that the devolved administrations and legislatures have the ability to make law in devolved policy areas as long as that law is compatible with EU law.

4.2 In areas where the devolved administrations and legislatures have competence, such as agriculture, environment and some transport issues, the devolved administrations and legislatures are responsible for implementing the common policy frameworks set by the EU. At EU level, the UK Government represents the whole of the UK's interests in the process for setting those common frameworks and these also then provide common UK frameworks, including safeguarding the harmonious functioning of the UK's own single market. When the UK leaves the EU, the powers which the EU currently exercises in relation to the common frameworks will return to the UK, allowing these rules to be set here in the UK by democratically-elected representatives.

4.3 As powers are repatriated from the EU, it will be important to ensure that stability and certainty is not compromised, and that the effective functioning of the UK single market is maintained. Examples of where common UK frameworks may be required include where they are necessary to protect the freedom of businesses to operate across the UK single market and to enable the UK to strike free trade deals with third countries. Our guiding principle will be to ensure that no new barriers to living and doing business within our own Union are created as we leave the EU.

4.4 To provide the greatest level of legal and administrative certainty upon leaving the EU, and consistent with the approach adopted more generally in legislating for the point of departure, the Government intends to replicate the current frameworks provided by EU rules through UK legislation. In parallel we will begin intensive discussions with the devolved administrations to identify where common frameworks need to be retained in the future, what these should be, and where common frameworks covering the UK are not necessary. Whilst these discussions are taking place with devolved administrations we will seek to minimise any changes to these frameworks. We will work closely with the devolved administrations to deliver an approach that works for the whole and each part of the UK.

4.5 This will be an opportunity to determine the level best placed to take decisions on these issues, ensuring power sits closer to the people of the UK than ever before. It is the expectation of the Government that the outcome of this process will be a significant increase in the decision making power of each devolved administration.

4.6 Legislation that is within the competence of the devolved legislatures or ministers giving effect to EU law will also need to be amended as we leave the EU. We therefore propose that the Bill also gives the devolved ministers a power to amend devolved legislation to correct law that will no longer operate appropriately, in line with the power we propose should be held by UK ministers.

Chapter 5: Crown Dependencies and Overseas Territories

5.1 The Crown Dependencies and the Overseas Territories, including Gibraltar, are not part of the UK for the purposes of EU law, nor are they separate members of the EU. However, they do have differing special statuses under the EU treaties.

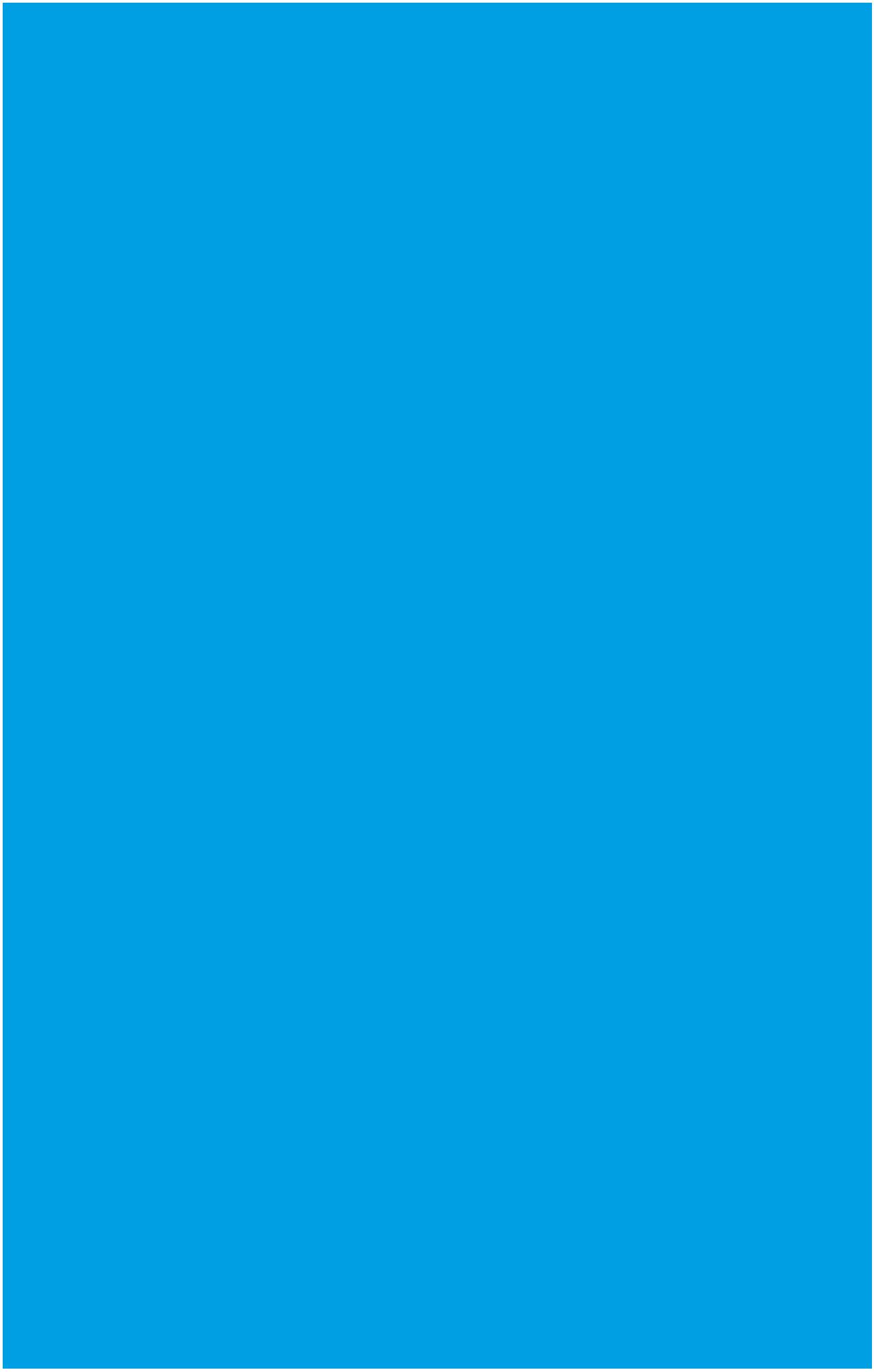
5.2 The Crown Dependencies are the Bailiwick of Jersey, the Bailiwick of Guernsey and the Isle of Man. Their relationship with the EU is set out in Protocol 3 to the UK's Act of Accession of 1972. As a general rule, the Crown Dependencies are not bound by EU law, but they are part of the customs territory of the EU. Therefore, EU customs matters, the common external tariff, levies, quantitative restrictions and any other measures having equivalent effect apply in the Crown Dependencies. There is free movement of agricultural goods and derived products between the islands and the EU.

5.3 Uniquely among the Overseas Territories, Gibraltar is largely subject to EU law. Under Article 355(3) TFEU, the treaties apply to Gibraltar as a European territory for whose external relations the UK is responsible. But there are some important exceptions, and certain provisions of EU law do not apply to Gibraltar under the UK's Act of Accession 1972. These include the provisions on the free movement of goods, the common commercial policy, the common agricultural policy, the common fisheries policy, and rules on VAT and other turnover taxes. Gibraltar is also outside the common customs territory and as a result EU rules on customs do not apply.

5.4 The EU treaties apply to a very limited extent in the other UK Overseas Territories (which are granted associate status under Part IV and Annex II of the TFEU) and the Sovereign Base Areas in Cyprus. For that reason the issues addressed in this White Paper in relation to preserving EU law do not arise for these territories to the same extent as they do for the Crown Dependencies and Gibraltar.

5.5 While the ECA applies to Gibraltar and the Crown Dependencies for certain purposes, each territory has its own equivalent legislation to give effect to the EU law which applies to it.

5.6 **The Government is committed to engaging with the Crown Dependencies, Gibraltar and the other Overseas Territories as we leave the EU.** We will continue to involve them fully in our work, respect their interests and engage with them as we enter negotiations, and strengthen the bonds between us as we forge a new relationship with the EU and look outward into the world. This includes technical engagement on any implications of the Great Repeal Bill for their jurisdictions.



Annex A: EU law in the UK

A.1 The Government's approach to preserving EU law is to ensure that all EU laws which are directly applicable in the UK and all laws which have been made in the UK in order to implement our obligations as a member of the EU are converted into domestic law on the day we leave the EU, subject to the exceptions set out in this paper. This chapter describes the different aspects of EU law in the UK.

The European Communities Act 1972

A.2 The ECA gives effect to the UK's obligations as a member of the EU and makes EU law supreme in the UK. The ECA will be repealed on the day we leave the EU, returning power to the UK Parliament.

A.3 As described in Chapter 2, some types of EU law (such as EU regulations and certain decisions) are directly applicable in the UK's legal system. This is provided for in section 2(1) of the ECA. Other types of EU law, such as directives, have to be given effect in UK law through national laws. Section 2(2) of the ECA provides ministers with a power to make secondary legislation for the purpose of implementing these EU obligations.

A.4 EU laws are sometimes given effect in UK law using primary legislation or using other powers to make secondary legislation instead of through secondary legislation made using the powers in section 2(2) of the ECA. Ministers in the devolved administrations also exercise powers to implement EU law in their areas of policy responsibility. Secondary legislation is the most common means by which the UK Parliament transposes EU directives into law.

The EU treaties

A.5 The EU treaties are the highest level of EU law. They define where the EU is permitted to act, to what extent and how. They also contain a mixture of procedural rules for how the EU operates and substantive rules, such as free movement rights for EU citizens. The EU treaties also set out subject areas in which the EU can make more specific laws: this is known as the EU's 'competence'.

A.6 The two main treaties are the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU). Some provisions of the TFEU have been found to be sufficiently clear, precise and unconditional that they confer rights directly on individuals. These are referred to as 'directly applicable' or 'directly effective' treaty provisions. Other treaty

provisions do not confer directly applicable rights but simply give the EU power to adopt legislation to give effect to the treaties' provisions.

The principle of supremacy of EU law

A.7 A key principle of EU law is that EU law is supreme, which means that it has the status of a superior source of law within the EU's member states. National laws must give way and be disapplied by domestic courts if they are found to be inconsistent with EU law. Notwithstanding, the UK Parliament is sovereign.

The general principles of EU law

A.8 General principles are part of the EU law with which the EU institutions and member states are bound to comply. General principles are applied by the CJEU and domestic courts when determining the lawfulness of legislative and administrative measures within the scope of EU law, and are also an aid to interpretation of EU law. Examples of general principles include non-retroactivity (i.e. that the retroactive effect of EU law is, in principle, prohibited) and the protection of legitimate expectations where, for example, an administrative decision is cancelled or revoked.

A.9 Currently, UK laws that are within the scope of EU law and EU legislation (such as directives) that do not comply with the general principles can be challenged and disapplied.

The Charter of Fundamental Rights

A.10 The Charter of Fundamental Rights sets out 'EU fundamental rights', which are general principles of EU law that have been recognised over time through the case law of the CJEU and which have been codified in the Charter which came into force in 2009. The Charter sets out 50 rights and principles, many of which replicate guarantees in the European Convention on Human Rights and other international treaties.

Directives, regulations and decisions

A.11 Below the treaties, the EU adopts directives, regulations and decisions using the powers, and following the procedures provided for, in the EU treaties.

A.12 Regulations contain detailed legal rules. Once made, regulations have the force of law in the UK and throughout the EU. Regulations only rarely require the member states to create their own legal rules in order to ensure the regulation has the desired legal effect. Examples of regulations include Regulation (EU) No 1143/2014 on the prevention and management of the introduction and spread of invasive alien species and Regulation (EC) No 726/2004 laying down procedures for the authorisation and supervision of medicinal products for human and veterinary use and establishing a European Medicines Agency.

A.13 Directives set out a legal framework that the member states have to follow, but leave it up to the member state to choose exactly how to make it part of their law. So, once an EU directive has been agreed, all member states have an obligation to make national laws that give it effect, but they have a choice as to precisely how to do so.

A.14 There are a variety of methods through which the UK has given effect to directives. The main methods are as follows:

a. Primary legislation. For example, the Equality Act 2010 contains provisions which give effect to various directives including Council Directive 2000/78/EC, which establishes a general framework for equal treatment in employment and occupation and Council Directive 2000/43/EC which implements the principle of equal treatment between persons irrespective of racial or ethnic origin.

b. Secondary legislation made under section 2(2) of the ECA. For example, the Energy Performance of Buildings (England and Wales) Regulations 2012 (S.I. 2012/3118), which give effect to parts of Directive 2010/31/EU of the European Parliament and of the Council on the energy performance of buildings.

c. Secondary legislation made under other primary legislation. For example, the Railways and Other Guided Transport Systems (Safety) Regulations 2006, which contain provisions implementing certain aspects of Directive 2004/49/EC (the Railway Safety Directive), are made under the Health and Safety at Work etc Act 1974 rather than under section 2(2) of the ECA.

A.15 The EU can also adopt binding decisions. Decisions may be addressed to a particular party or parties, which could be individuals (including companies) or member states. For example, the Commission has powers to issue decisions that are binding in order to enforce competition rules.[14]

A.16 Below regulations, decisions and directives which are made using one of the EU legislative procedures, the EU also adopts measures in order to supplement and amend, or to implement, the rules set out in directives, regulations or decisions. Such measures are referred to respectively as 'delegated' and 'implementing' acts. For example, under Article 4 of Regulation (EU) No 1143/2014 on the prevention and management of the introduction and spread of invasive alien species, the European Commission adopts implementing acts in order to list plant species which are assessed as invasive alien species for the purposes of the Regulation.

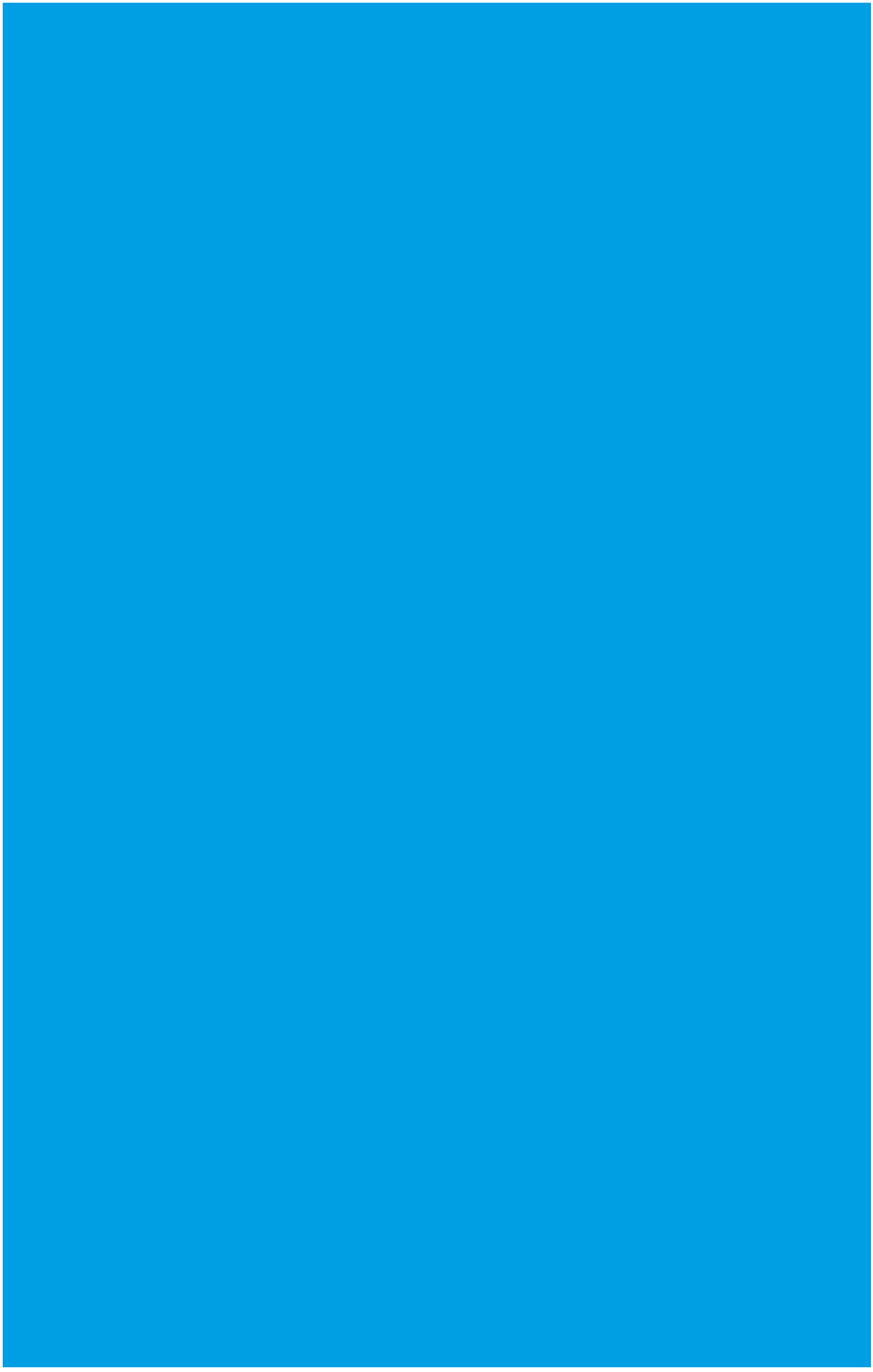
EU case law

A.17 In addition to the EU legal instruments described above, the case law of the CJEU also forms part of EU law. The CJEU has jurisdiction to rule on the interpretation and application of the EU treaties. In particular, the Court has jurisdiction to rule on challenges to the validity of EU acts, in infraction proceedings brought by the Commission against member states and on references from national courts concerning the interpretation of EU acts.

Recommendations and opinions

A.18 Recommendations and opinions are non-binding legal acts issued by the EU institutions. They are not legally binding on member states but can be used as an aid to interpretation by domestic courts when interpreting EU law.

[14] See, for example, decisions adopted by the Commission in 2007 in relation to certain car manufacturers – http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007D0788&from=EN



Glossary

Term	Definition
Act of Parliament	An Act of Parliament is a law that both Houses of Parliament have agreed to, and which is enforced in all the areas of the UK where it is applicable.
Bill	A proposal for a new law or an amendment to an existing law that has been presented to Parliament for consideration. Once agreed and made into law, it becomes an Act.
Charter of Fundamental Rights	The Charter of Fundamental Rights sets out 'EU fundamental rights' which is a term used to describe human rights as they are recognised in EU law. EU fundamental rights are general principles of EU law which have been recognised over time through the case law of the CJEU and which have been codified in the Charter which came into force in 2009. The Charter sets out 50 rights and principles, many of which replicate guarantees in the European Convention on Human Rights and other international treaties. See Article 6 TEU.
Coming into force	The process by which an Act of Parliament, secondary legislation or other legal instrument comes to have legal effect. The law can be relied upon from the date on which it comes into force but not any sooner. Also known as commencement.
Competence	Competence means all the areas where the treaties give the EU the ability to act, including the provisions in the treaties giving the EU institutions the power to legislate, to adopt non-legislative acts, or to take any other sort of action. It also means areas where the treaties apply directly to the member states without needing any further action by the EU institutions. The EU's competences are set out in the EU treaties, which provide the basis for any actions the EU institutions take. The EU can only act within the limits of the competences conferred on it by the treaties, and where the treaties do not confer competences on the EU they remain with the member states. See Article 5(2) TEU.

Converted EU-derived law	EU laws that applied in the UK the moment before the UK left the EU, which are converted into domestic law through the Great Repeal Bill.
Court of Justice of the European Union (CJEU)	The CJEU has jurisdiction to rule on the interpretation and application of the treaties. In particular, the Court has jurisdiction to rule on challenges to the validity of EU acts, in infraction proceedings brought by the Commission against member states and on references from national courts concerning the interpretation of EU acts. The Court is made up of two sub-courts: the General Court and the Court of Justice (which is sometimes called the ECJ). See Article 19 TEU and Articles 251 to 281 TFEU.
Decision	A legislative act of the EU which is binding upon those to whom it is addressed. If a decision has no addressees, it binds everyone. See Article 288 TFEU.
Delegated Act	A form of EU delegated instrument. A legislative act, such as a directive or a regulation, can delegate power to the Commission to adopt delegated acts to supplement or amend non-essential elements of the legislative act. See Article 290 TFEU.
Directive	A legislative act of the EU which requires member states to achieve a particular result without dictating the means of achieving that result. Directives must be transposed into national law using domestic legislation, in contrast to regulations, which are enforceable as law in their own right. See Article 288 TFEU.
EU agencies	EU agencies are legal entities (separate from the EU institutions) set up to perform specific tasks under EU law. They include bodies such as the European Medicines Agency, the European Police Office (Europol) and the European Union Agency for Railways.
EU institutions	There are a number of EU bodies which are defined under the Treaties as EU institutions including the European Parliament, the European Council, the Council of the European Union and the European Commission.
The EU Treaties (including TEU and TFEU)	The European Economic Community (EEC) was established by the Treaty of Rome in 1957. This Treaty has since been amended and supplemented by a series of treaties, the latest of which is the Treaty of Lisbon. The Treaty of Lisbon, which entered into force on 1 December 2009, re-organised the two treaties on which the European Union is founded: the Treaty on European Union (TEU) and the Treaty establishing the European Community, which was re-named the Treaty on the Functioning of the European Union (TFEU).

European Commission	The Commission is the main executive body of the EU. It has general executive and management functions. In most cases it has the sole right to propose EU legislation. In many areas it negotiates international agreements on behalf of the EU and represents the EU in international organisations. And the Commission also oversees and enforces the application of Union law, in particular by initiating infraction proceedings where it considers that a member state has not complied with its EU obligations. See Article 17 TFEU and Articles 244 to 250 TFEU.
European Convention on Human Rights (ECHR)	An international convention, ratified by the United Kingdom and incorporated into UK law in the Human Rights Act 1998. It specifies a list of protected Human Rights, and establishes a Court (European Court of Human Rights sitting in Strasbourg) to determine breaches of those rights. All member states are parties to the Convention. The Convention is a Council of Europe Convention, which is a different organisation from the EU. Article 6 TEU provides for the EU to accede to the ECHR.
European Council	The European Council defines the general political direction and priorities of the EU. It consists of the Heads of State or Government of the Member States, together with its President and the President of the Commission. See Article 15 TEU and Articles 235 and 236 TFEU.
European Parliament	The European Parliament (EP) consists of representatives elected by Union citizens. The EP shares legislative and budgetary power with the Council, and has oversight over the actions of the Commission. See Article 14 TEU and Articles 223 to 234 TFEU.
Implementing acts	A form of EU delegated instrument. A legislative act, such as a directive or a regulation, can enable the Commission (and in some cases the Council) to adopt implementing acts where uniform conditions for implementing the legislative act are needed. See Article 291 TFEU.
Regulation	A legislative act of the EU which is directly applicable in member states without the need for national implementing legislation (as opposed to a directive, which must be transposed into national law by member states using domestic legislation). See Article 288 TFEU.
Secondary legislation	Legal instruments (including regulations and orders) made under powers delegated to ministers or other office holders in Acts of Parliament. They have the force of law but can be disapplied by a court if they do not comply with the terms of their parent Act. Also called subordinate or delegated legislation.
Statute book	The body of legislation that has been enacted by Parliament or one of the devolved legislatures and has effect in the UK.
Statutory instrument	A form of secondary legislation to which the Statutory Instruments Act 1946 applies.

ISBN 978-1-4741-4005-8

Appendix 4:

House of Lords report of European Union Committee:

Brexit: the EU data protection package

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

Appendix 5:

UK Government Report

The exchange and protection of personal data

HM Government

The exchange and protection of personal data

A FUTURE PARTNERSHIP PAPER

The United Kingdom wants to build a new, deep and special partnership with the European Union.

This paper is part of a series setting out key issues which form part of the Government's vision for that partnership, and which will explore how the UK and the EU, working together, can make this a reality.

Each paper will reflect the engagement the Government has sought from external parties with expertise in these policy areas, and will draw on the very extensive work undertaken across Government since last year's referendum.

Taken together, these papers are an essential step towards building a new partnership to promote our shared interests and values.

The exchange and protection of personal data: a future partnership paper

Executive summary

1. Data flows are important for the UK and the EU economies and for wider cooperation, including on law enforcement matters. To ensure that individuals have control over and transparency as to how their personal data is being used, and that their personal data is protected from misappropriation and misuse, robust safeguards are needed.

2. The UK has strong domestic personal data protection standards, set out in the Data Protection Act (DPA) 1998. The UK's new Data Protection Bill, which will repeal and replace the DPA 1998, was announced in this year's Queen's Speech. It will further strengthen UK standards, ensuring they are up to date for the modern age, and it will implement the EU's new data protection framework in our domestic law. At the point of our exit from the EU, the UK's domestic data protection rules will be aligned with the EU data protection framework.

3. After leaving the EU, the UK will continue to play a leading global role in the development and promotion of appropriate data protection standards and cross-border data flows. In doing so we will work alongside the EU and other international partners to ensure that data protection standards are fit for purpose – both to protect the rights of individuals, but also to allow businesses and public authorities to offer effective services and protect the public.

4. After the UK leaves the EU, new arrangements to govern the continued free flow of personal data between the EU and the UK will be needed, as part of the new, deep and special partnership. The UK starts from an unprecedented point of alignment with the EU. In recognition of this, the UK wants to explore a UK-EU model for exchanging and protecting personal data, which could build on the existing adequacy model, by providing sufficient stability for businesses, public authorities and individuals, and enabling the UK's Information Commissioner's Office (ICO) and partner EU regulators to maintain effective regulatory cooperation and dialogue for the benefit of those living and working in the UK and the EU after the UK's withdrawal.

Introduction

5. The Commission has highlighted the value of the EU data economy, which was estimated to be worth €272 billion in 2015, or around two per cent of EU GDP. It has grown rapidly in recent years.[1] External estimates suggest that its value could rise to €643 billion by 2020, more than three per cent of GDP, as long as policy and legal frameworks for the data economy are put in place.[2]

[1] 'Building a European Data Economy', European Commission, January 2017.
[2] Ibid.

6. Increasingly, data flows envelop all trade in goods and services as well as other business and personal relations. The UK is a significant player in global data flows. Estimates suggest that around 43 per cent of all large EU digital companies are started in the UK[3], and that 75 per cent of the UK's cross-border data flows are with EU countries.[4] Analysis indicates that the UK has the largest internet economy as a percentage of GDP of all the G20 countries[5], and has an economy dominated by service sectors in which data and data flows are increasingly vital. The UK accounted for 11.5 per cent of global cross-border data flows in 2015, compared with 3.9 per cent of global GDP and 0.9 per cent of global population[6], but the value of data flows to the whole economy and the whole of society are greater still.

7. Any disruption in cross-border data flows would therefore be economically costly to both the UK and the EU. Taking EU-US data flows as a comparator, external estimates suggest that if cross-border data flows between the EU and the US were seriously disrupted, the EU's GDP could reduce by between 0.8 and 1.3 per cent.[7] Therefore, placing restrictions on cross-border data flows could harm both the economies of the countries implementing these policies, as well as others in the global economy.

8. Sharing personal data is also essential for wider cooperation that helps in the fight against serious crime and terrorism. The sharing of personal data is crucial to the EU's ongoing work across the continent to protect citizens, in which the UK plays an integral role. For example, between October 2014 and September 2015, the UK Financial Intelligence Unit (UKFIU) received 1,566 requests from international partners for financial intelligence. Of these, at least 800 came from EU Member States. In the same period, the UKFIU proactively disseminated 571 pieces of financial intelligence to international financial intelligence units, 200 of which went to Europol.[8] This intelligence contains personal data relating to individuals, companies and bank accounts suspected of connection with money laundering, terrorist financing and other financial crime. Well-designed, strong data protection standards go hand in hand with supporting innovative uses of data.

9. While personal data flows support both the UK and EU economies and the UK's wider cooperation with the EU, including on law enforcement matters, effective protections must be in place to ensure that data relating to individuals ('personal data') is handled appropriately and properly protected against any misuse, including when this data is transferred to another country.

---

[3] 'The Digital Economy', Business, Innovation and Skills Committee, House of Commons, July 2016.

[4] 'The UK digital sectors after Brexit', Frontier Economics, January 2017.

[5] 'The Internet Economy in the G20', Boston Consulting Group, March 2012.

[6] 'The UK digital sectors after Brexit', Frontier Economics, January 2017.

[7] 'The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce', European Centre for International Political Economy (ECIPE), March 2013.

[8] 'Suspicious Activity Reports (SARs) Annual Report 2015', National Crime Agency, March 2016.

Context

10. Recent technological advances have led to huge increases in the amount of personal data being processed and transferred, including across borders. Over time this has necessitated the development of more robust rules to:

    - protect personal data from being stolen or disclosed to those without authorisation;
    - prevent personal data from being misused by those who have access to it; and
    - keep personal data accurate, particularly where automatic decisions are being taken which have an impact on people, such as those concerning pensions, insurance, or creditworthiness.

11. In the UK, it has long been established that personal information should be protected in certain contexts. Doctors are expected to protect confidential information about their patients, and lawyers about their clients. Principles such as these existed long before any law dedicated to data protection was passed. The development of UK legislation on data protection can be traced back to at least 1970 and the establishment of the Younger Committee, and the UK's Data Protection Act 1984 was in place before the EU legislated in this area.

12. When the UK updated its data protection law to implement the EU Data Protection Directive 1995 (the 1995 Directive), it extended the rights and obligations beyond the minimum required by EU law. For example, the UK's update to the data protection law (DPA 1998) ensured that the same standards applied to certain types of law enforcement processing which were not covered by the 1995 Directive.

The EU data protection framework

13. The EU has recently updated its existing data protection framework (the 1995 Directive), in the form of a new General Data Protection Regulation (GDPR). This covers general processing of personal data within the scope of EU law, and a separate Data Protection Directive (DPD) relating to personal data being processed for law enforcement purposes. The UK played a full and active part in negotiations for the new GDPR and DPD, and the final text reflects a number of key UK priorities. For instance, the GDPR takes a more risk-based approach than had previously been adopted, with the result that certain obligations with which data controllers must comply are proportionate to the risk posed by the data processing activity. The GDPR and DPD were adopted in 2016 and are due to come into force in May 2018 (replacing the 1995 Directive), before the UK leaves the EU. The new rules strengthen rights and empower individuals by giving them more control over their personal data.[9]

14. The EU data protection framework includes mechanisms governing data flows between Member States and third countries.

    - All European Economic Area (EEA) states are directly party to the GDPR. For this reason, data can be transferred freely between EEA states without the need for businesses and public authorities to satisfy themselves in each case that the relevant national data protection safeguards are sufficient.

[9] 'Reform of EU data protection rules', European Commission, May 2016.

- For non-EEA countries, the EU data protection framework includes provisions allowing the Commission to decide that a third country's data protection framework is 'adequate', which allows data to flow freely between the EEA and those third countries. The existing adequacy model is discussed in paragraphs 32-41. Alternatives to adequacy are also available under the EU framework, but these can be more costly and onerous for businesses and public authorities, and are more limited in their application; Annex A sets out the alternatives to adequacy in more detail.

15. The GDPR will apply to processing of personal data that takes place in third countries outside of the EEA if it is related to the offering of goods or services to individuals in the EEA, or monitoring their behaviour. As such, UK businesses and public authorities may still be required to meet GDPR standards for their processing of EEA personal data following the date of withdrawal.[10]

16. The Government announced its plans in the Queen's Speech for a new UK Data Protection Bill which will replace the DPA 1998. This will ensure that the UK's framework is aligned with the updated EU legal framework at the date of withdrawal. The Government published its Statement of Intent on the Bill on 7 August 2017, setting out its proposed approach to the legislation in more detail.[11]

Other international data protection standards

17. The Council of Europe's Data Protection Convention (Convention 108) is a source of high-level data protection principles. It was signed in 1981 and is less detailed than the EU framework, which it pre-dates. Convention 108 is currently being modernised, in part to bring it more into line with the new EU data protection framework. Its high-level approach is likely to remain the same following completion of the modernisation process, although it is expected that there will be increased specificity in some provisions. The UK's data protection standards will remain fully aligned with the revised Convention 108.

18. Other international organisations have also noted the need for their own data protection principles. For example:

- the Organisation for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were adopted in 1980 and were updated in 2013 – they seek to harmonise national privacy legislation while preventing interruptions in international free flows of data; and

- the Asia Pacific Economic Forum Privacy Framework was adopted in 2005, recognising the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and support economic growth in the Asia Pacific region.

[10] See Article 3: Territorial Scope.
[11] 'A New Data Protection Bill: Our Planned Reforms', DCMS, 7 August 2017.

Outline of UK objectives

19. The UK recognises the need for, and is one of the leading drivers of, high data protection standards across the globe. An appropriate balance must be maintained between individuals' right to privacy and control over their own data, the ability of individuals, companies and other organisations to share data to create services which consumers value, and the ability of law enforcement bodies to protect citizens from crime and terrorism.

20. In an ever more connected world, we cannot expect data flows to remain confined within national borders. Moves towards data localisation, or the Balkanisation of the internet, risk stifling the competition, innovation and trade which produce better services for consumers, and can weaken data security. Global leadership and standards are needed to ensure that individuals can have confidence that their data is being appropriately protected wherever they choose to access goods or services, but not in such a way as to undermine the provision of those goods or services, including on a cross-border basis.

21. It is therefore the UK's ambition to remain a global leader on data protection, by promoting both the flow of data internationally and appropriate high levels of data protection rules. Case law demonstrates that there are divergent views globally on how to strike the right balance. The UK has played an important role in developing the EU's approach to data protection, including by playing a full part in the negotiation of the GDPR and DPD: throughout this process we promoted a balanced approach between freedoms and protections. The UK wants to continue to work closely with the EU, which has also been at the forefront of driving the improvement of global data protection standards, and our wider international partners, to work towards stronger global standards.

22. Underpinning this, as the UK and the EU build a new, deep and special partnership, it is essential that we agree a UK-EU model for exchanging and protecting personal data, that:

- maintains the free flow of personal data between the UK and the EU;
- offers sufficient stability and confidence for businesses, public authorities and individuals;
- provides for ongoing regulatory cooperation between the EU and the UK on current and future data protection issues, building on the positive opportunity of a partnership between global leaders on data protection;
- continues to protect the privacy of individuals;
- respects UK sovereignty, including the UK's ability to protect the security of its citizens and its ability to maintain and develop its position as a leader in data protection;
- does not impose unnecessary additional costs to business; and
- is based on objective consideration of evidence.

This could build on the existing adequacy model.

A UK-EU model for exchanging and protecting personal data between the UK and the EU, and beyond

23. A UK-EU model for exchanging and protecting personal data should recognise that the UK is compliant with EU data protection law and wider global data protection standards, and that the UK will introduce a Data Protection Bill which will, among other things, implement the GDPR and the DPD. In light of the UK's unprecedented position, the future deep and special partnership between the UK and the EU could productively build on the existing adequacy model (which is set out in more detail in paragraphs 32-41) in two key respects.

Regulatory co-operation

24. **After the UK's withdrawal, regulatory cooperation between the UK and the EU on a range of issues will be essential, including data protection** – not least because the GDPR will continue to apply to UK businesses offering goods or services to individuals in the EEA. A new relationship could therefore enable an ongoing role for the UK's ICO in EU regulatory fora, preserving existing, valuable regulatory cooperation and building a productive partnership to tackle future challenges.

25. The ICO works closely with other EU regulators and is well-regarded amongst its EU and international counterparts. Its resources and experience are a part of an established and effective EU regulatory dynamic. As the UK's data protection authority, the ICO plays an active role in helping determine the practical application of EU data protection law within EU fora.

26. A continued role for the ICO will support cross-border business and activity between the UK and the EU by promoting a common understanding of the regulatory challenges and issues faced by businesses, the public sector and individuals. The UK would be open to exploring a model which allows the ICO to be fully involved in future EU regulatory dialogue. An ongoing role for the ICO would allow the ICO to continue to share its resources and expertise with the network of EU Data Protection Authorities, and provide a practical contribution at EU level which will benefit citizens and organisations in both the UK and the EU. Indeed, this responds to the Commission's call to develop international co-operation mechanisms to facilitate effective cooperation and enforcement of data laws by data supervisory authorities.[12] The UK Government will continue to have responsibility for the content and direction of data protection policy and legislation within the United Kingdom.

Certainty and stability

27. In light of the existing alignment of our data protection frameworks, the UK also believes that a UK-EU model for exchanging and protecting personal data could provide an opportunity to give greater **ongoing certainty** to business and citizens in both the UK and the EU as to the rules governing future data flows, reducing the risks for business that the basis for data flows is unexpectedly changed.

---

[12] 'Exchanging and Protecting Personal Data in a Globalised World', European Commission, January 2017.

28. When the UK leaves the EU, it is essential that we avoid regulatory uncertainty for businesses and public authorities in the UK, EEA, and EU adequate countries who currently enjoy an ability to transfer data freely. Uncertainty over the nature of the data relationship between the UK and EU immediately on exit may force businesses on both sides to incur unnecessary expense and time in contingency planning, or put them under pressure to renegotiate what may be less favourable contractual arrangements. Ensuring certainty at the point of exit will avoid unnecessary disruption for businesses, public authorities and individuals in the UK and EU.

29. The UK's data protection law fully implements the EU framework, and this will remain the case at the point of our exit from the EU. On this basis, the Government believes it would be in the interest of both the UK and EU **to agree early in the process to mutually recognise each other's data protection frameworks** as a basis for the continued free flows of data between the EU (and other EU adequate countries) and the UK from the point of exit, until such time as new and more permanent arrangements come into force.

30. Early certainty around how we can extend current provisions, alongside **an agreed negotiating timeline for longer-term arrangements**, will assuage business concerns on both sides and should be possible given the current alignment of our data protection frameworks.

31. As well as ensuring that data flows between the UK and the EU can continue freely, the UK also wants to make sure that **flows of data between the UK and third countries with existing EU adequacy decisions can continue** on the same basis after the UK's withdrawal, given such transfers could conceivably include EU data. The UK is, and will remain after the point of withdrawal, a safe destination for personal data with some of the strongest domestic data protection standards in the world. For this reason, the UK does not see any reason for existing data flows from third countries to the UK to be interrupted. The UK will liaise with those third countries to ensure that existing arrangements will be transitioned over at the point of exit.

Existing EU processes and arrangements for international data flows

32. The 1995 Directive allows the Commission to formally recognise that a third country provides an 'adequate' level of data protection under EU law. Third countries do not formally agree or sign up to these decisions, although they are generally informed by prior discussions between the Commission and the third country regarding their domestic data protection law. Any areas where the Commission requires reassurance will require negotiation between the parties on how best to address the issues.

33. Adequacy decisions allow businesses and public authorities to continue to transfer data from the EEA to respective third countries without having to satisfy themselves that adequate safeguards are in place for each transfer.

34. Under current arrangements, any third country can request the Commission considers them for an adequacy decision. If it wishes, the Commission can then assess whether the nature of that country's data protection rules and the means for ensuring their effective supervision and enforcement, are sufficient to provide an adequate level of protection.

35. In making its assessment of a third country's data protection rules, the Commission will scrutinise that country's domestic legislation and practice, as well as compliance with relevant international standards, in order to ascertain whether the data protection standards in the third country are 'essentially equivalent' to those applied in the EU (a test set by the CJEU in Schrems).[13]

36. There is no set timeframe for the adequacy decision process. Once proposed, the decision needs to be confirmed by a panel of representatives from EU Member States, and the Commission can revoke the adequacy decision in the future. Adequacy decisions may also be invalidated by the CJEU.

37. To date, the Commission has adopted 12 adequacy decisions under the existing 1995 Directive, with: Andorra, Argentina, Canada (for transfers to commercial organisations who are subject to the Canadian Personal Information Protection and Electronic Documents (PIPED) Act), the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and the US (for certified companies). All are subject to routine review.

38. As well as adequacy decisions covering all transfers of personal data to a third country, partial adequacy decisions can be made covering only certain sectors of the economy. As mentioned above, two of the EU's current adequacy decisions are partial: the Canada Decision applies only to transfers of data to Canadian recipients who are subject to the PIPED Act; and the EU-US Privacy Shield is a different type of partial adequacy, in that it applies only to transfers to those companies in the US that have self-certified as having met the standards set out in the Privacy Shield framework. Various factors have, to date, been considered in determining whether to grant a partial or sector-specific adequacy decision (rather than a full decision), including whether there is an overarching data protection law in the third country, its constitutional structure and whether certain of its sectors are particularly exposed to data flows from the EU.

[13] Maxmillian Schrems v Data Protection Commissioner (C-362/14), Grand Chamber, 6 October 2015.

39. The new GDPR and DPD each contain adequacy provisions. Both measures amend some elements of the existing adequacy framework, providing a lot more detail on the elements the Commission must consider when coming to an adequacy decision. These include the rule of law, respect for human rights and fundamental freedoms, any international commitments entered into, and the third country's relevant legislation. The new framework also states that adequacy decisions should be reviewed periodically, and at least every four years.

40. On 10 January 2017, the Commission published a communication setting out its strategy for engaging selected third countries to reach adequacy decisions, starting with Japan and South Korea. It recently announced plans to conclude its adequacy decision with Japan by early 2018. This stems from a desire to achieve progress in the ongoing EU-Japan trade deal negotiations.

41. The new EU data protection framework also sets out a number of legal bases other than adequacy for transferring personal data to countries outside the EEA (see Annex A). Once the new framework has come into force, businesses and public authorities operating within and outside of the EEA will need to have one or more of these arrangements in place to underpin their transfers of personal data to non-EEA countries that do not have an EU adequacy decision. However, simply extending these provisions or establishing new ones to cover personal data transfers between the UK and the EU would be more burdensome for businesses and public authorities in both the UK and the EU, and would represent a missed opportunity to build a new partnership that reflects the close alignment of our data protection frameworks.

Conclusion

42. After leaving the EU, the UK will continue to play a leading global role in the development and promotion of appropriate data protection standards and cross-border data flows. In doing so we will work alongside the EU and other international partners to ensure that data protection standards are fit for purpose – both to protect the rights of individuals, but also to allow businesses and public authorities to offer effective services and protect the public.

43. Data flows between the UK and the EU are crucial for our shared economic prosperity and for wider cooperation, including on law enforcement. It is therefore essential that as part of the UK's future partnership with the EU, we agree arrangements that allow for free flows of data to continue, based on mutual trust in each other's high data protection standards.

44. Given that the UK will be compliant with EU data protection law and wider global data protection standards on exit, and given the important role of continued regulatory cooperation as part of a future economic relationship, the UK believes that a UK-EU model for exchanging and protecting personal data could provide for regulatory cooperation and ongoing certainty for businesses and public authorities. This could build on the existing adequacy model.

45. The UK's data protection law will fully implement the most up-to-date EU framework, and this will remain the case at the point of the UK's withdrawal from the EU. On this basis, the Government believes it would be in the interest of both the UK and EU to agree early in the process to mutually recognise each other's data protection frameworks as a basis for the continued free flows of data between the EU (and other EU adequate countries) and UK from the point of exit until such time as new and more permanent arrangements come into force.

46. As we leave the EU, the Government will also work with the devolved administrations and the governments of Gibraltar, the other Overseas Territories and the Crown Dependencies as we progress negotiations with the EU. We will continue to work closely with these governments on the detail of these proposals as they affect their interests.

Annex A: the alternatives to adequacy under the GDPR and DPD

1. Without an adequacy decision or new model in place, it is still possible for personal data to be transferred to third countries in some circumstances. In addition to various limited derogations from the general requirements, both the GDPR and the DPD set out alternative methods of transfer, which companies and public authorities may use to transfer data to third countries in the absence of an adequacy decision.

2. Under the GDPR, alternative legal bases for transfers of personal data outside the EEA include:

   - **Binding Corporate Rules** that allow the transfer of data between the establishments of a company located inside and outside the EU;

   - **Standard Contractual Clauses** that data controllers can adopt as the basis for data transfers; and

   - **Approved Codes of Conduct**, or approved certification mechanisms.

3. However, none of these alternatives are as wide ranging as an adequacy decision or an agreed new relationship. They can also be costly and onerous for businesses, especially for small and medium sized enterprises (SMEs).

   - Companies may need to pay for legal advice on what alternatives would be most appropriate.

   - Many companies may need their own customised contractual clauses drafted. These can be expensive and must be submitted for approval by EU regulators, which may take some time. Standard Contractual Clauses, as drafted by the Commission, do not require any approval but are inflexible and may not suit a particular company's processing situation.

   - Alternatively, businesses in the EEA wishing to transfer personal data to a UK branch could set up a Binding Corporate Rule. These also need approval by EU regulators and leading legal firms have indicated that on average they cost around £250,000 to set up.

   - Codes of conduct and certification mechanisms are insufficient by themselves: they must be accompanied by binding and enforcing commitments, which will entail legal costs, and must be approved by the European Data Protection Board.

4. Under the DPD, transfers to a third country or international organisation for law enforcement purposes are permitted in the absence of an adequacy decision. However, unless a derogation applies, this only applies where appropriate safeguards have been provided in a legally binding instrument, for instance, for a legally binding bilateral agreement between countries. Transfers can also occur in the absence of an adequacy decision where the controller has assessed all the circumstances and considers that appropriate safeguards exist.

5. Derogations for transfers in specific situations are also provided for in the DPD, but these are limited, for example, to protect the vital interests of the data subject or another person, or for the prevention of an immediate and serious threat to public security of a Member State or a third country. However, the ability to use these alternatives and derogations is more limited than adequacy.

Appendix 6:

EU

Position paper on the Use of Data and Protection of Information Obtained or Processed before the withdrawal date

20 September 2017

TF50 (2017) 14/2 – Commission to UK

Subject: Position paper on the **Use of Data and Protection of Information Obtained or Processed before the withdrawal date**

Origin: European Commission, Task Force for the Preparation and Conduct of the Negotiations with the United Kingdom under Article 50 TEU

Remarks: The attached position paper on the **Use of Data and Protection of Information Obtained or Processed before the withdrawal date** contains the main principles of the EU position in this regard

Published on Thursday 21 September on the TF50 website as EU position in view of the 4th negotiation round with the UK

Essential Principles on the Use of Data and Protection of Information Obtained or Processed before the Withdrawal Date

It is recalled that the United Kingdom's access to networks, information systems and databases established by Union law is, as a general rule, terminated on the date of withdrawal.

The United Kingdom or entities in the United Kingdom may keep and continue to use data or information received/processed[1] in the United Kingdom before the withdrawal date and referred to below only if the conditions set out in this paper are fulfilled. Otherwise such data or information (including any copies thereof) should be erased or destroyed.

The principles set out in this paper should also apply, *mutatis mutandis*, to personal data, data or information which was received /processed by the United Kingdom or entities in the United Kingdom after the withdrawal date pursuant to the Withdrawal Agreement.

I. Protection of personal data processed before the withdrawal date

The following general principles should apply in accordance with Union law, as interpreted by the Court of Justice of the European Union on the date of entry into force of the Withdrawal Agreement:

(1) The provisions of Union law on personal data protection[2] applicable on the withdrawal date should continue to apply to personal data in the United Kingdom processed before the withdrawal date and pertaining to

(i) data subjects in the EU27,

(ii) data subjects outside the Union,

to the extent that this data is covered by Union law on personal data protection before the withdrawal date.

The data subjects concerned should, for example, continue to have the right to be informed, the right of access, the right to rectification, to erasure, to restriction of processing, to data portability as well as the right to object to processing and not to be subject to a decision based solely on automated processing, on the basis of relevant provisions of Union law applicable on the withdrawal date. Personal data referred to above should be stored no longer than is necessary for the purposes for which the personal data was processed; it should be erased afterwards. Where sectorial rules applicable on the withdrawal date provide for specific maximum mandatory storage periods, the data should be automatically erased upon the expiry of that period. The personal data in question could only be transferred to non-EU27 countries and to international organizations if the transfer is carried out in accordance with the conditions set forth in Union law on personal data

[1] Article 4(2) of 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 (General Data Protection Regulation) defines processing as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

[2] The General Data Protection Regulation, 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, as well as other Union legal instruments containing provisions on personal data protection.

protection applicable on the withdrawal date, in particular Chapter V of Regulation (EU) 2016/679.

The data subjects concerned should also be able to enforce their rights in accordance with the relevant provisions of Union law applicable on the withdrawal date, in particular Chapter VIII of Regulation (EU) 2016/679, for as long as the personal data in question continues to be processed in the United Kingdom after the withdrawal date.

(2) Personal data of data subjects in the United Kingdom processed before the withdrawal date by the Union institutions, agencies, offices and bodies or in the EU27 will continue to be protected in accordance with the Union law applicable on the withdrawal date.

(3) The Withdrawal Agreement should allow for the orderly completion of investigations or procedures for the monitoring of compliance with personal data protection provisions between the United Kingdom authorities and EU27 authorities or Union institutions, agencies, offices and bodies (such as the European Data Protection Board) which are ongoing on the withdrawal date, in particular those provided for in Chapter VII of Regulation (EU) 2016/679.

II. Protection of EUCI[3] and national classified information[4] exchanged in the interests of the EU before the withdrawal date

The following general principles should apply in accordance with Union law, as interpreted by the Court of Justice of the European Union on the withdrawal date:

(1) EUCI and national classified information received from EU27 Member States or Union institutions, agencies, offices and bodies before the withdrawal date by the United Kingdom on the basis of Union law, should continue to be protected in accordance with the provisions of Union law applicable on the withdrawal date, in particular Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information, Commission Decision 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, as well as the Agreement of 4 May 2011 between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union. The same applies to information received from the United Kingdom before the withdrawal date by EU27 Member States or Union institutions, agencies, offices and bodies.

(2) The United Kingdom should continue to ensure that contractors and subcontractors as well as grant beneficiaries registered in its territory take all appropriate measures to protect EUCI and national classified information when performing a classified contract[5] or classified grant

[3] According to Article 2 of Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information: "'*EU classified information' (EUCI) means any information or material designated by a EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States*".

[4] According to Article 2 of the Agreement of 4 May 2011 between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union, "'*classified information' shall mean any information or material, in any form, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States, and which bears one of the […] EU classification markings or a corresponding classification marking as set out in the Annex".*

[5] A contract the performance of which requires or involves the creation, handling or storing of EUCI (see Commission Decision 2015/444 of 13 March 2015, Article 40(a))

agreement[6] concluded with a Union contracting authority or Union granting authority before the withdrawal date.

(3) The United Kingdom should continue to ensure, in accordance with national laws and regulations, that contractors or subcontractors as well as grant-beneficiaries registered in its territory participating in classified contracts or classified grant agreements concluded with a Union contracting authority or Union granting authority before the withdrawal date which require access to EUCI or national classified information within their facilities in the performance of such contracts or agreements hold a Facility Security Clearance at the relevant classification level.[7]

(4) The Withdrawal Agreement should allow for the orderly completion of procedures between the United Kingdom authorities and EU27 authorities or Union institutions, agencies, offices and bodies which are ongoing on the withdrawal date, as regards the protection of EUCI or national classified information, in particular security investigations. It should also allow for the possibility to start and conduct, after the withdrawal date, cooperation procedures relating to the protection of classified information exchanged before the withdrawal date.

(5) The UK shall notify the EU of any incident or change in policy regarding the approval of cryptographic products used for the protection of EUCI.

III. Other restrictions of use and access to data and information obtained before the withdrawal date

The following general principle should apply in accordance with Union law, as interpreted by the Court of Justice of the European Union on the withdrawal date:

Data and information received by the United Kingdom from EU27 Member States, Union institutions, agencies, offices and bodies, or private entities established in the EU27, before the withdrawal date, which are subject to Union rules restricting the use or access to such data and information (e.g. access or purpose restrictions, limitations of storage periods) other than those referred to in sections I and II on the withdrawal date, should continue to be protected in accordance with the provisions in Union law restricting the use or access to such data and information applicable on the withdrawal date. The same principle should apply to data and information received by EU27 Member States or Union institutions, agencies, offices and bodies from the United Kingdom or entities established therein, before the withdrawal date.

Examples of such Union rules restricting the use or access to data and information other than those referred to in sections I and II include:

- Rules concerning the protection of information of the kind covered by the obligation of professional secrecy obtained in the context of Union merger, antitrust or State aid procedures;
- Rules concerning regulatory data protection of pre-clinical, clinical, and toxicological (human health and environment) studies as well as other data submitted in accordance with applicable Union law;
- Rules concerning the protection of information acquired by customs authorities.

[6] An agreement whereby the granting authority awards a grant the performance of which requires or involves the creation, handling or storing of EUCI (see Commission Decision 2015/444 of 13 March 2015, Article 40(c)).

[7] It is recalled that the withdrawal of a Facility Security Clearance by the United Kingdom would constitute sufficient grounds for the contracting or granting authority, to terminate a classified contract or grant agreement concerned.

Appendix 7:

EU Commission

NOTICE TO STAKEHOLDERS
WITHDRAWAL OF THE UNITED KINGDOM FROM THE UNION AND EU RULES IN THE FIELD OF DATA PROTECTION

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS

Brussels, 9 January 2018

NOTICE TO STAKEHOLDERS

WITHDRAWAL OF THE UNITED KINGDOM FROM THE UNION AND EU RULES IN THE FIELD OF DATA PROTECTION

The United Kingdom submitted on 29 March 2017 the notification of its intention to withdraw from the Union pursuant to Article 50 of the Treaty on European Union. This means that unless a ratified withdrawal agreement[1] establishes another date, all Union primary and secondary law will cease to apply to the United Kingdom from 30 March 2019, 00:00h (CET) ('the withdrawal date').[2] The United Kingdom will then become a 'third country'.[3]

In view of the considerable uncertainties, in particular concerning the content of a possible withdrawal agreement, all stakeholders processing personal data are reminded of legal repercussions, which need to be considered when the United Kingdom becomes a third country.[4]

Subject to any transitional arrangement that may be contained in a possible withdrawal agreement, as of the withdrawal date, the EU rules for transfer of personal data to third countries apply. Aside from an "adequacy decision", which allows the free flow of personal data from the EU without the EU data exporter having to implement any additional safeguards or being subject to further conditions, the EU's data protection rules (both under the current Directive 95/46 and under the new General Data Protection Regulation 2016/679, "GDPR" - which will apply as from 25 May 2018) allow a transfer if the controller or processor has provided "appropriate safeguards". These safeguards may be provided for by:

---

1 Negotiations are ongoing with the United Kingdom with a view to reaching a withdrawal agreement.

2 Furthermore, in accordance with Article 50(3) of the Treaty on European Union, the European Council, in agreement with the United Kingdom, may unanimously decide that the Treaties cease to apply at a later date.

3 A third country is a country not member of the EU.

4 For the continued application of EU safeguards of personal data processed while the United Kingdom was a Member State, the Commission has published an essential principles paper here: https://ec.europa.eu/commission/publications/position-paper-use-data-and-protection-information-obtained-or-processed-withdrawal-date_en.

- **Standard data protection clauses:** the Commission has adopted three sets of model clauses which are available on the Commission's website;[5]
- **Binding corporate rules:** legally binding data protection rules approved by the competent data protection authority which apply within a corporate group;
- Approved **Codes of Conduct** together with binding and enforceable commitments of the controller or processor in the third country;
- Approved **certification mechanisms** together with binding and enforceable commitments of the controller or processor in the third country.

In the absence of an "adequacy decision" or of "appropriate safeguards" a transfer or a set of transfers may take place on the basis of so-called **"derogations"**: they allow transfers in specific cases, such as based on consent, for the performance of a contract, for the exercise of legal claims or for important reasons of public interest.

These tools are well-known to business operators in the Member States, as they are already being used today for the transfers of personal data to non-EU countries.

The GDPR has simplified the use of these tools by cutting red tape compared to the current Directive 95/46. Transfers based on approved standard data protection clauses or on binding corporate rules will not be subject to a further, specific authorisation from a supervisory authority. In addition, the GDPR has, subject to further conditions, introduced codes of conduct and certification mechanisms as new tools for the transfer of personal data.

Preparing for the withdrawal is not just a matter for EU and national authorities but also for private parties. As regards the implementation of the GDPR, and in particular the new tools for transfers to third countries (e.g. approved Codes of Conduct and approved certification mechanisms entailing binding commitments by the controllers and processors receiving the data in the third country), the Commission (DG JUST) is working with interested parties and data protection authorities to make the best use of these new instruments. Moreover, the Commission has set up a stakeholder group comprised of industry, civil society and academics, in which this topic will be discussed.

European Commission
Directorate-General Justice and Consumers

[5] https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

Appendix 8:

EU Data Processing Supervisor

Note on Personal Data Transfers After Brexit

EUROPEAN DATA PROTECTION SUPERVISOR

Information note on international data transfers after Brexit

16 July 2019

1. Background information

According to the current state of play, the UK including Northern Ireland will leave the EU on 1 November 2019 at 00.00 am CET and will become a third country[1].

In case the EU and the UK sign the withdrawal agreement (Title VII), as negotiated by the end of 2018, before 1 November 2019, the data flows to the UK will not be immediately affected. The withdrawal agreement provides for the application of EU data protection law until 31 December 2020, and this period may be extended for another two years. The General Data Protection Regulation (GDPR), the law enforcement Directive (EU) 2016/680, the ePrivacy Directive and any other provisions governing the protection of personal data are considered as Union data protection law.

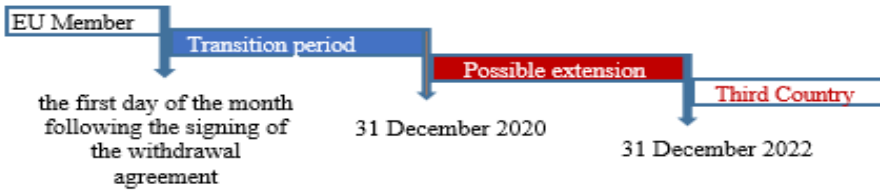


Fig. 1 Timeline foreseen in the Withdrawal Agreement

However, a no-deal Brexit scenario would have repercussions for the protection of personal data. This is because the EU primary and secondary law, including the data protection law, will cease to apply in the UK. Personal data transfers to the UK will be subject to specific conditions with which Union institutions and bodies (EUIs) need to comply. Some institutions and bodies are already familiar with the available data transfer mechanisms, as they are already transferring data to third countries outside the EEA.

Fig. 2 Timeline in case of a no-deal Brexit

The EDPS builds upon the guidance provided on this matter by the European Commission and by the European Data Protection Board.

[1] On the 7 May 2019, the UK government confirmed that it will hold European Parliament elections and therefore the UK will not leave the EU on 1 June 2019.

2. Data transfers from Union institutions and bodies to the UK in case of no-deal Brexit

In case of a no-deal Brexit the flow of data from EUIs to the UK and Northern Ireland will be subject to the requirements for international data transfers as laid down in Chapter V of Regulation (EU) 2018/1725 (EU DPR). For example, if an EUI outsources mission trips management or IT services to a processor in the UK, legal safeguards will be required for the personal data transferred to the UK.

2.1. International data transfers mechanisms

The EU DPR provides that a data transfer to a third country, such as the UK, shall not undermine the level of protection guaranteed by this Regulation (Article 46). This level of protection shall be maintained for onward transfers, i.e. transfers from the third country, such as the UK, to another third country or international organisation. For this purpose, the EU DPR lays down a series of mechanisms which the controllers and processors may choose to enable the transfer to a third country. It is up to them to assess which of the available mechanisms best reflects their situation.

2.1.1 Adequacy decisions

A transfer of personal data to a third country can take place when the European Commission has recognized this third country as offering an adequate level of protection (Article 47). The effect of such an adequacy decision is that personal data can flow from the EUIs to that third country as if the transfer takes place within the EU/EEA.
However, no such recognition of the UK legal framework will be in place before the UK leaves the EU and relevant negotiations will require time.
Therefore, EUIs shall consider adopting other transfer mechanisms from the ones provided in Chapter V.

2.1.2 Appropriate safeguards

There are a series of data transfer mechanisms adducing appropriate safeguards. Article 48 EU DPR lists all ‘appropriate safeguards’. A common feature of all is the condition that they must provide for enforceable and effective data subjects rights.

a. Instruments exclusively available to public authorities

EUIs as public authorities may consider to use the mechanisms which the EU DPR considers more apt to their situation (Article 48(2)(a) and (3)(b)).
One option is to use a legally binding and enforceable instrument, such as an administrative agreement, a bilateral or multilateral international agreement. The agreement must be binding and enforceable for the signatories.
The second option is to use administrative arrangements, such as Memoranda of Understanding. Although not legally binding themselves, they shall however provide for enforceable and effective data subject rights. The non-binding administrative arrangements are subject to an authorisation by the EDPS.

b. Standard Data Protection Clauses

In case EUIs are interacting with private entities (for instance, outsourcing mission trips management, IT services or training)[2], they may consider signing standard data protection clauses adopted by the European Commission. These contracts offer the additional adequate safeguards with respect to data protection that are needed in case of a transfer of personal data to any third country.
Three sets of standard data protection clauses are currently available (remaining valid under the GDPR until amended, replaced or repealed by a Commission decision):

- EU controller to third country (non EU/EEA) controller (e.g. UK): 2 Sets are available:
  - 2001/497/EC
  - 2004/915/EC
- EU controller to third country (non EU/EEA) processor (e.g. UK):
  - 2010/87/EC

It is important to note that the standard data protection clauses may not be modified and must be signed as provided. However, these contracts may be included in a wider contract and additional clauses might be added provided that they do not contradict, directly or indirectly, the standard data protection clauses adopted by the European Commission[3].
Any further modifications to the standard data protection clauses will imply that this will be considered as ad-hoc contractual clauses which will require a prior authorisation by the EDPS (analysed under e).
Finally, the EU DPR provides for the possibility of standard data protection clauses adopted by the EDPS and approved by the Commission. So far such clauses have not been adopted.

c. Binding Corporate Rules

Binding Corporate Rules are personal data protection policies adhered to by a group of undertakings (ie. multinationals) in order to provide appropriate safeguards for transfers of personal data within the group, including outside of the EU/EEA.
In case the processor of a specific activity is not an EUI, he may already make use of BCRs for processors (these binding corporate rules apply to data received from a controller established in the EU, which is not a member of the group, and then processed by the concerned group members as processors and/or sub-processors)[4]. BCRs authorised under the former Directive 95/46/EC remain valid under the GDPR (Article 46(5)) and are considered as a transfer mechanism adducing adequate safeguards according to the EU DPR (Art. 48(2)(d)). However, they need to be updated in order to be fully in line with the GDPR provisions.
Future Binding Corporate Rules must be approved by the competent national supervisory authority, following an opinion of the EDPB (Article 47(1) and 64(3) GDPR), prior to any transfer.

d. Codes of conduct and certification mechanisms

[2] EDPS, The transfer of personal data to third countries and international organisations by EU institutions and bodies, Position Paper, p. 20-22.
[3] See the following communication of the European Commission http://europa.eu/rapid/press-release_MEMO-05-3_en.htm.
[4] Article 29 Data Protection Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev. 1, 28 November 2017, available on the EDPB website.

In the event that the processor is not an EUI, codes of conduct or certification mechanisms, as provided in GDPR, can be used in order to offer appropriate safeguards for transfers to a third country.
These tools are new under GDPR and therefore the work of the EDPB, which is currently working on guidelines in order to further clarify the content and the use these tools, should be closely followed.

e. Ad hoc contractual clauses

In case EUIs are interacting with private entities, they can also make use of ad-hoc contractual clauses they negotiate with UK counterparts in order to provide appropriate safeguards taking into account their particular situation.
Prior to any transfer, these tailored contractual clauses must be authorised by the EDPS (Art. 48(3)(a) EU DPR).

2.1.3 Derogations [5]

In the absence of an adequacy decision, EUIs should first consider providing adequate safeguards, framing the transfer of personal data with one of the mechanisms mentioned under 2.1.2.

Derogations provided in Article 50 EU DPR are exemptions from the general principle that personal data may only be transferred to third countries if an adequate level of protection is provided for in the third country or if appropriate safeguards have been adduced and the data subjects enjoy enforceable and effective rights. Furthermore, transfers based on a derogation are not required to have any kind of prior authorisation from the EDPS, leading to increased risks for the rights and freedoms of the data subjects concerned. Therefore, derogations must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive.

Derogations are exhaustively mentioned in Article 50(1) EU DPR and include data transfers:

- where an individual has explicitly consented to the proposed transfer after having been provided with all necessary information about the risks associated with the transfer;
- where the data transfer is necessary for the performance of a contract to which a data subject is a part or for the implementation of pre-contractual measures;
- where the data transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- where the data transfer is necessary for important reasons of public interest;
- where the data transfer is necessary for the establishment, exercise or defence of legal claims;
- where the data transfer is necessary for the protection of the vital interests of the data subject or of other persons and the data subject is physically or legally incapable of giving consent and

[5] See also EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, regarding the similar provisions of the General Data Protection Regulation (GDPR).

- where a transfer is made from a public register.

3. Data transferred before the withdrawal date

The European Commission in the Position Paper on the Use of Data and Protection of Information Obtained or Processed before the withdrawal date concludes that UK based controllers and processors may continue to process personal data transferred before the withdrawal date only if these data enjoy the protection of EU data protection law. Such protection will be guaranteed, in case that a Withdrawal Agreement is put in place.

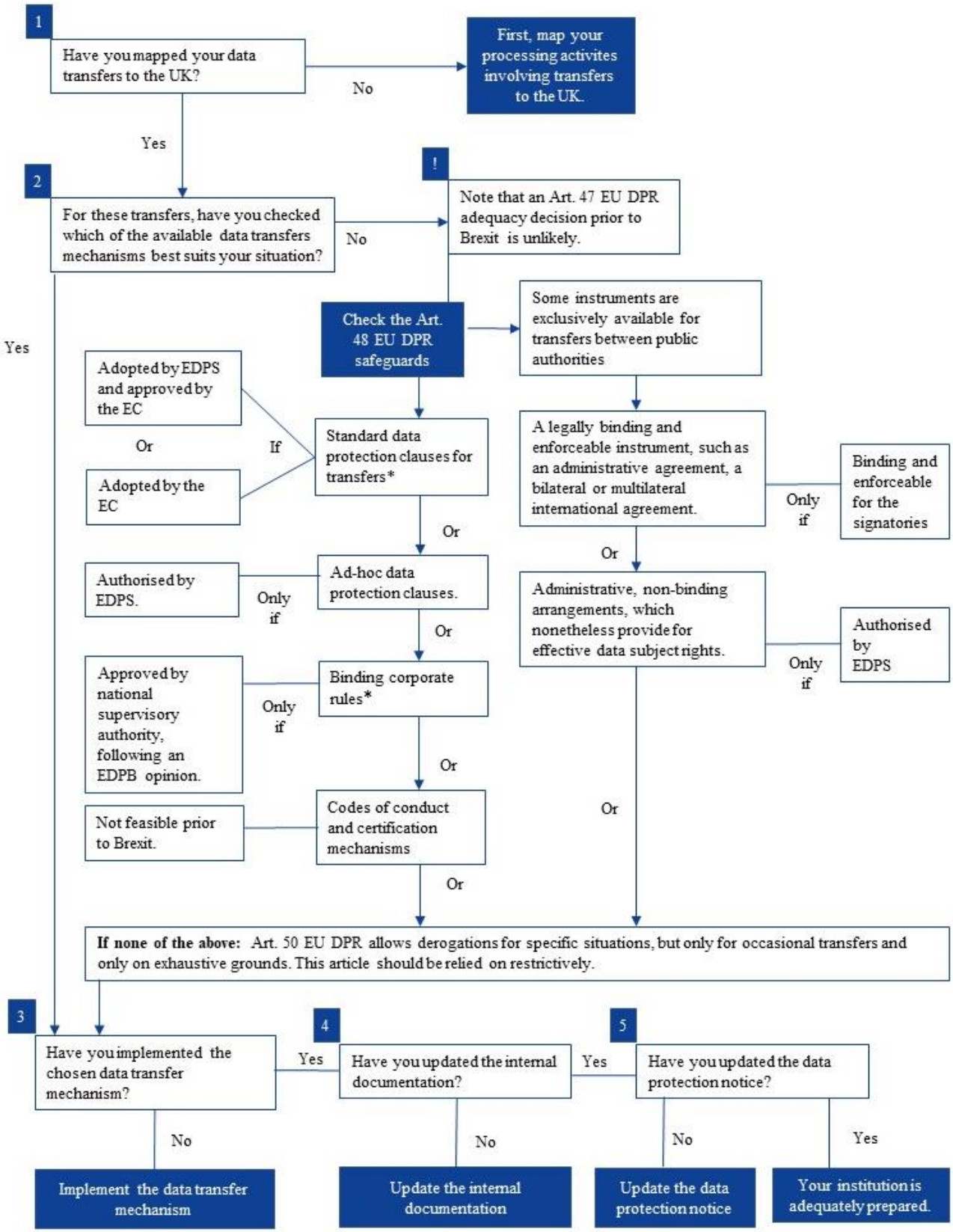
The developments on this sensitive issue should be closely followed and the EDPS may provide further guidance if is deemed necessary.

4. Steps to take in order to be prepared

In order to be prepared for the case of no-deal Brexit, EUIs should take the following steps:

i. map their processing activities;
ii. check the available data transfers mechanism that best suits their situation;
iii. implement the chosen data transfer mechanism before 1 June or 1 November 2019;
iv. update their internal documentation;
v. update their data protection notice accordingly.

4.1. In brief: steps to take in order to be prepared for a no-deal Brexit



* Binding corporate rules and standard contractual clauses (adopted by the EC) under the old Directive 95/46 are still valid, but will need to be updated over time in line with the GDPR. In any case, before using old EC standard contractual clauses you should make sure to adapt them to Regulation (EU) 2018/1725 [EU DPR].