HOUSE OF COMMONS LIBRARY

BRIEFING PAPER

Number 7838, 10 October 2017

Brexit and data protection

By John Woodhouse and Arabella Lang

Contents:

Contents

Summary

The EU data protection framework

The main piece of EU data protection law is the 1995 Data Protection Directive. The Directive was implemented into UK law by the *Data Protection Act 1998*. The 1998 Act provides the legal framework for data protection in the UK.

A 2008 Council Framework Decision applies to the processing of personal data in police and judicial cooperation in criminal matters. This was transposed into UK law by the *Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014*.

The EU's Charter of Fundamental Rights and Freedoms is also now central to EU data protection law, with a number of cases relying on Charter Article 8 in preference to other EU data protection provisions.

Since 1995, digital technology has profoundly changed the way data is collected, accessed and used. In addition, Member States have implemented the 1995 rules differently, resulting in divergences in enforcement. In January 2012, the European Commission therefore proposed a new legislative framework for data protection. In its now finalised form, this has two elements:

- The General Data Protection Regulation ("GDPR")
- The Police and Criminal Justice Directive ("PCJ Directive", also known as the "Law Enforcement Directive")

The GDPR will apply in the UK from 25 May 2018.

The PCJ Directive must be transposed into national law by 6 May 2018.

Third countries

Under the EU's data protection framework, any country other than the EU and EEA Member States is classed as a "third country".

Personal data can only be transferred to a third country when an adequate level of protection is guaranteed. One option is for the European Commission to make an "adequacy decision" so that data can flow from EU/EEA Member States to third countries (or one or more specific sectors in those countries). Other options include binding corporate rules and standard contractual clauses.

Data protection after Brexit

On leaving the EU, the UK would become a third country.

The Government has stressed that it wants to maintain the unhindered flow of data between the UK and the EU after Brexit. However, in a July 2017 report, the Lords Select Committee on the European Union said it was "struck by the lack of detail on how the Government plans to deliver this outcome". The Committee recommended that the Government should seek adequacy decisions as "the least burdensome and most comprehensive platform for sharing data with the EU" after Brexit. It warned of a "cliff-edge" if transitional arrangements did not allow for continuity of data sharing.

Some business leaders have also expressed concern at what will happen after Brexit.

In an August 2017 position paper, the Government said that it "wanted to explore a UK-EU model for exchanging and protecting personal data that could build on the existing adequacy model."

The *Data Protection Bill [HL] 2017-19* will bring the GDPR and PCJ Directive into UK law and, according to the Government, "ensure that the UK is prepared for the future after we have left the EU".

However, the Government proposes to exclude the Charter of Fundamental Rights from 'EU retained law' after Brexit. Instead, underlying rights and principles will be carried forward and will be substitute reference points in pre-Brexit case-law referring to the Charter.

This raises a number of questions for data protection. For instance:

- How could EU data protection law be read so as to replace references to Article 8 of the Charter with references to other data protection law?
- How would the UK continue close cooperation with the EU on exchanging data, when compliance with the Charter is likely to be required in practice to ensure regulatory equivalence?

1. The EU data protection framework

The main piece of EU data protection law is the 1995 Data Protection Directive.[1] The Directive was implemented into UK law by the *Data Protection Act 1998*. The 1998 Act provides the legal framework for data protection in the UK.

A 2008 Council Framework Decision applies to the processing of personal data in police and judicial cooperation in criminal matters.[2] This was transposed into UK law by the *Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014*.[3]

The EU's Charter of Fundamental Rights and Freedoms is also now central to EU data protection law, with a number of cases relying on Charter Article 8 in preference to other EU data protection provisions. The Charter is discussed more fully in section 2.4 of this paper.

Since 1995, digital technology has profoundly changed the way data is collected, accessed and used. In addition, Member States have implemented the 1995 rules differently, resulting in divergences in enforcement. In January 2012, the European Commission therefore proposed a new legislative framework for data protection.[4] In its now finalised form, this has two elements:

- The General Data Protection Regulation ("GDPR")[5]
- The Police and Criminal Justice Directive ("PCJ Directive", also known as the "Law Enforcement Directive")[6]

The European Commission website has a range of material on the reforms.

1.1 The General Data Protection Regulation (GDPR)

The GDPR came into force on 24 May 2016. As a Regulation, it will have direct application in Member States. There is a two-year transition period for implementation. The Government has said that the GDPR will apply in the UK from 25 May 2018.[7]

The Regulation sets out the responsibilities of "data controllers" (the bodies that determine the purposes and means of processing of

1 Directive 95/46/EC
2 Framework Decision 2008/977/JHA
3 SI 2014/3141. 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 Treaty on the Functioning of the European Union (TFEU). For further legislative background see the Explanatory Memorandum to SI 2014/3141.
4 See the Library Briefing Paper, *The draft EU Data Protection Framework*, June 2013
5 Regulation 2016/679 EU
6 Directive 2016/680/EU
7 Department for Culture, Media and Sport, *Call for views on the General Data Protection Regulation derogations*, April 2017, p1

personal data) and "data processors" (those who process personal data on behalf of a controller). It also sets out the rights of "data subjects" (the individuals whose personal data is being processed).

The Regulation does not extend to activities that fall outside the scope of EU law (e.g. national security). The processing of personal data for law enforcement purposes will be covered by the new Police and Criminal Justice Directive.

According to a European Commission factsheet, the GDPR will "strengthen citizens' rights and build trust". It will also help businesses in the Digital Single Market through the "clarity and consistency" of the rules that will apply.[8]

Changes made by the GDPR

The GDPR has an increased territorial scope. It applies to "the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not."[9]

The Regulation also applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or
- the monitoring of their behaviour as far as their behaviour takes place within the EU.[10]

After Brexit, the GDPR will therefore continue to apply to UK companies who process data in ways that bring them within its scope, even if they are not established inside the EU.

Other changes include:

- **Data protection by design and default** – data protection safeguards should be built into systems from the earliest stage of development.[11]
- A **European Data Protection Board** will be set up to ensure the consistent application of the Regulation. It will consist of representatives of the 28 independent supervisory authorities. The Board will replace the existing Article 29 Committee.[12]
- **Increased penalties** - organisations can be fined up to 4% of annual global turnover or €20 Million (whichever is greater).[13]

---

8 European Commission, Questions and Answers - Data protection reform package, 24 May 2017
9 Article 3(1)
10 Article 3(2)
11 Article 25
12 Article 68
13 Article 83

- **Data protection officers** - all public authorities and companies performing certain data processing operations will need to appoint a data protection officer.[14]
- A **"one-stop shop"** principle – allowing companies with subsidiaries in several member states to deal with the data protection authority in the member state of its main establishment.

Data subjects' rights

The GDPR will enhance the rights of data subjects in a number of ways. These include:

- **Strengthened conditions for consent** – consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of their personal data.[15] Consent can be withdrawn at any time.[16]
- **Right of access –** data subjects will have the right to obtain confirmation from a data controller as to whether or not their personal data is being processed, where and for what purpose.[17]
- **Right to erasure ("right to be forgotten") –** data subjects will have the right to obtain from a data controller the erasure of personal data if certain conditions are met e.g. the data no longer being relevant to original purposes for processing, or the data subject withdrawing consent. The right does not apply if processing is necessary for the right of freedom of expression or for reasons of public interest.[18]
- **Data portability** – data subjects will have the right to receive and transmit their personal data to other controllers (when it has been previously provided in a commonly used and machine readable format).[19]
- **Breach notification** - breach notification will become mandatory where a data breach is likely to result in a "high risk to the rights and freedoms" of data subjects.[20]

Parental consent will be required to process the personal data of children under the age of 16 for online services. Member states can legislate for a lower age of consent but this will cannot be below the age of 13.[21]

14 Article 37
15 Article 4(11), Recital 32
16 Article 7(3)
17 Article 15
18 Article 17
19 Article 20
20 Article 34
21 Article 8

The Regulation promotes techniques such as pseudonymisation (replacing personally identifiable material with artificial identifiers) to protect personal data.[22]

In the UK, the Information Commissioner's Office (ICO) has started to publish material on the GDPR. This includes an overview of the Regulation, guidance for businesses, and a "myth busting" blog.

1.2 The Police and Criminal Justice Directive (PCJ Directive)

The PCJ Directive came into force on 5 May 2016. EU Member States are required to transpose it into their national law by 6 May 2018.

According to the European Commission, the Directive will protect the personal data of individuals involved in criminal proceedings, whether as witnesses, victims, or suspects. In addition it will "facilitate a smoother exchange of information between Member States' police and judicial authorities, improving cooperation in the fight against terrorism and other serious crime in Europe".[23]

Changes made by the Directive

The 2008 Framework Decision only applies to cross-border data processing and not to processing activities by the police and judiciary authorities at purely national level. According to the European Commission, this created difficulties for police and other competent authorities who "are not always able to easily distinguish between purely domestic and crossborder processing or to foresee whether certain personal data may become the object of a cross-border exchange at a later stage".[24]

The PCJ Directive will apply to both cross-border and domestic processing of personal data within the scope of EU law.

Other changes introduced by the Directive include:

- New rights of access and information for data subjects
- Data protection 'by design and by default'
- Right to erasure
- Data breach notifications
- Data Protection Officers[25]

---

22 Article 4(5), Recitals 28 and 29

23 European Commission, Questions and Answers - Data protection reform package, 24 May 2017

24 European Commission, COM(2012) 10 final, 25 January 2012, p2

25 See European Commission website, *The directive on protecting personal data processed for the purpose of criminal law enforcement* (Archived 27/9/2016), Accessed 6 October 2017; House of Lords European Union Committee, *Brexit: the EU data protection package*, HL Paper 2017-19, 18 July 2017, pp15-6

1.3 "Third countries"

Under the EU's data protection framework, any country other than the EU and EEA Member States is classed as a "third country".

Personal data can only be transferred to a third country when an adequate level of protection is guaranteed. One option is for the European Commission to make an "adequacy decision" so that data can flow from EU/EEA member states to third countries (or one or more specific sectors in those countries).

Other options include binding corporate rules and standard contractual clauses.

Further detail on transfers to third countries and international organisations is available from the ICO website and the European Commission website.

2. Data protection after Brexit

Summary

The Government has stressed that it wants to maintain the unhindered flow of data between the UK and the EU after Brexit.[26]

However, in a July 2017 report, the Lords Select Committee on the European Union said it was "struck by the lack of detail on how the Government plans to deliver this outcome".[27]

Some business leaders have also expressed concern at what will happen after Brexit.[28]

The Lords Committee recommended that the Government should seek adequacy decisions as "the least burdensome and most comprehensive platform for sharing data with the EU" after Brexit.[29] It warned of a "cliff-edge" if transitional arrangements did not allow for continuity of data sharing.

In an August 2017 position paper, the Government said that it "wanted to explore a UK-EU model for exchanging and protecting personal data that could build on the existing adequacy model."[30]

The *Data Protection Bill [HL] 2017-19* will bring the GDPR and PCJ Directive into UK law and, according to the Government, "ensure that the UK is prepared for the future after we have left the EU".[31]

However, the Government proposes to exclude the Charter of Fundamental Rights from 'EU retained law' after Brexit. This raises a number of questions for data protection, including whether compliance with the Charter is likely to be required in practice to ensure regulatory equivalence after leaving the EU.

2.1 The UK as a third country

On leaving the EU, the UK would become a "third country" (section 1.3 above). Earlier this year, the House of Lords Select Committee on the European Union took evidence on what would then happen.

The Committee asked Rosemary Jay (a lawyer and academic on data protection) how straightforward it would be to negotiate an adequacy agreement with the EU. She pointed out that this required a "formal, legislative decision" and couldn't be done in an informal way:

---

26 Matt Hancock (Minister for Digital) oral evidence to the Select Committee on the European Union Home Affairs Sub-Committee, 1 February 2017, p1

27 House of Lords European Union Committee, *Brexit: the EU data protection package*, HL Paper 2017-19, 18 July 2017, p3

28 See, for example, "Brexit: Business and security risks of leaving EU data sharing scheme 'not on Tories' radar', experts warn", *Independent*, 3 June 2017; "CBI warns of cliff edge for £240bn data economy", *City AM*, 13 September 2017

29 House of Lords European Union Committee, *Brexit: the EU data protection package*, p50

30 HM Government, *The exchange and protection of personal data: a future partnership paper*, August 2017, p2

31 DCMS, *Data Protection Bill Factsheet – Overview*, September 2017, p1

> (…) an adequacy decision is a formal, legislative decision of the EU. The Commission actually has to make that decision. It has to go through a legislative process. It is not simply within its gift to do it in some informal way…I can see no way that that could be foreshortened. An adequacy decision is a decision made in relation to a third country. Technically, I do not think we can get to adequacy in that sense before we become a third country. It just seems logically that we cannot do that. There is a legislative barrier. I cannot comment on whether there is some procedural mechanism such that the process is expedited the day we walk out. In my view, it would be optimistic but I am happy to take other people's views.[32]

According to Stewart Room (global head of cybersecurity and data protection legal services at PricewaterhouseCoopers), an adequacy decision would give "certainty to businesses and to the economy".[33] He observed that in Brexit negotiations there would be a shared interest with the EU in maintaining strong data protection:

> (…) The essential point about data protection is that all of Europe, regardless of the nature of the EU, believes in this subject matter…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 this country afterwards. If you are a French-headquartered multinational, for instance, you would want to ensure that the French Government achieved the same form of data protection in this country…[34]

On data protection after Brexit, Valsamis Mitsilegas (Professor of European Criminal Law at QMUL) noted the role of the Court of Justice:

> 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 EU law after the entry into force of the Lisbon treaty. This means that compatibility, equivalence 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, while you can say it has an advisory role, in reality, when the assessment is made, the Court of Justice's case law must be taken into account.[35]

What did the Lords Committee conclude?

In its July 2017 report the Committee supported the Government's objective of securing uninterrupted data flows between the UK and the EU post-Brexit. However it was "struck by the lack of detail on how the Government plans to deliver this outcome".[36] The Committee urged the Government to set out its plans as soon as possible.[37]

One of the Committee's conclusions was that the most effective way to achieve unhindered data flows after Brexit would be through adequacy

---

32 Oral evidence to the Select Committee on the European Union Home Affairs Sub-Committee, 1 March 2017, p8
33 Ibid, p7
34 Ibid, p8
35 Ibid, p10
36 House of Lords European Union Committee, *Brexit: the EU data protection package*, p50
37 Ibid, p50

decisions from the European Commission. Although other legal mechanisms existed, it would be difficult for the UK to get by without an adequacy arrangement - three-quarters of the UK's cross-border data flows are with EU countries. The Committee recommended 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.[38]

The Committee warned of a "cliff-edge" if any transitional arrangements did not allow for continuity of data sharing.[39]

In the field of data protection, the Committee said that there was no prospect of a "clean break" from the EU:

> 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.
>
> 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.

The Committee also warned of a possible loss of UK influence:

> 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.
>
> 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.[40]

---

38 Ibid, p50
39 Ibid, p50
40 Ibid, p51

2.2 The Government's future partnership paper (August 2017)

In August 2017, the Government published a future partnership paper on the exchange and protection of personal data after Brexit. According to the paper, the Government wants to explore a UK-EU model for exchanging and protecting personal data that could build on the existing adequacy model:

> (…) 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.[41]

2.3 European Commission position paper (September 2017)

In September 2017, the European Commission published a position paper setting out the main principles of the EU position on the use and protection of data obtained or processed before the UK's withdrawal:

> 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 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…

In general, the paper will provide for the continuity of the principles of the EU data protection framework to personal data processed in the UK before withdrawal date.[42]

The Court of Justice of the European Union (CJEU) will interpret the general principles referred to in the paper.

2.4 Data protection and the EU Charter of Fundamental Rights

Summary

The EU's Charter of Fundamental Rights and Freedoms is now central to EU data protection law, with a number of cases relying on Charter Article 8 in preference to other EU data protection provisions.

---

41 HM Government, *The exchange and protection of personal data: a future partnership paper*, August 2017, p2

42 Elif Mendos Kuşkonmaz, 'Brexit and Data Protection: The Tale of the Data Protection Bill and UK-EU Data Transfers', EU Law Analysis blog, 26 September 2017

The Government proposes to exclude the Charter from 'EU retained law' after Brexit. Instead underlying rights and principles will be carried forward and will be substitute reference points in pre-Brexit case-law referring to the Charter.

This raises a number of questions for data protection. For instance:

- How could EU data protection law be read so as to replace references to Article 8 of the Charter with references to other data protection law?
- How would the UK continue close cooperation with the EU on exchanging data, when compliance with the Charter is likely to be required in practice to ensure regulatory equivalence?

Why is the Charter relevant?

The Charter now has a central role in EU law on data protection and data processing. Article 8 of the Charter contains a wide and freestanding right to the protection of personal data:

> **Protection of personal data**
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. 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.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

Although this is based partly on the predecessor to Article 16 TFEU (right to data protection)[43] and the 1995 Data Protection Directive,[44] it appears to go further than other EU legislation. It also goes further than the equivalent provision of the European Convention on Human Rights.[45]

Since the Charter gained EU treaty status in 2009, many decisions of the Court of Justice of the EU (CJEU) and the UK courts have relied on its provisions. A series of successful and ongoing legal challenges to EU-third country and EU internal data protection instruments demonstrate how active a role the Charter plays in EU data protection and data-sharing law. For instance, in a recent opinion on an EU-Canada agreement on transferring personal data outside the EU,[46] the Grand Chamber of the Court of Justice said that it would refer only to Charter

43 Article 286 of the EC Treaty
44 Directive 95/46/EC
45 ECHR Article 8. See David Davis and others v Secretary of State for the Home Department [2015] EWHC 2092 (Admin) para 80: "Article 8 of the Charter clearly goes further, is more specific, and has no counterpart in the ECHR".
46 Opinion 1/15 on the transfer of Passenger Name Record data from the European Union to Canada, 26 July 2017 (Grand Chamber)

Article 8 because that provision lays down the conditions of data processing in a more specific manner than Article 16 TFEU.[47]

The Government's proposal for the Charter

The European Union (Withdrawal) Bill currently before the House of Commons provides in clause 5(4) that 'the Charter of Fundamental Rights is not part of domestic law on or after exit day'. This is one of the few specified exceptions to the Bill's aim of continuity of EU law.

The Government considers that the Charter would not be 'relevant' after Brexit, because it applies to the UK only when acting 'within the scope' of EU law, and asserts that no substantive rights will be lost as a result of not retaining it.

Indeed, under clauses 2, 3 and 4 of the Bill, much EU data protection law would be retained in UK law and could continue to be relied on in UK courts.

Further, clause 5(5) states that references to the Charter in the pre-Brexit case-law of either the CJEU or UK domestic courts are to be read as if they were references to the corresponding 'fundamental rights or principles' that are considered to exist irrespective of the Charter.

And 'general principles of EU law' recognised by the CJEU, including on data protection, would be retained, but only for the purposes of interpreting other retained EU law (clause 6(7) and Schedule 1 paras 2 and 3).

What might be the data protection implications of removing the Charter from UK law?

Despite the retention of other data protection law, there are several potential implications for data protection if the Charter is removed. For instance:

- Would any aspects of the Charter right to data protection be lost because they are not reflected in EU retained law or other enforceable law in the UK?
- How could data protection case-law be read so as to replace references to Article 8 of the Charter with references to other data protection law?[48]
- How would references in the GDPR to the Charter be dealt with? (The GDPR's Recitals refer to Article 8 and the substantive provisions refer to the Article 47 right to an effective remedy.)
- What if the 'corresponding' right derives from EU secondary legislation that has not been properly implemented in UK law?
- How would the UK continue close cooperation with the EU on exchanging data,[49] when compliance with the Charter is likely to

---

47 See Lorna Woods (Professor of Internet Law, University of Essex), 'Transferring personal data outside the EU: Clarification from the ECJ?', EU Law Analysis blog, 4 August 2017

48 See Professor Steve Peers, 'The White Paper on the Great Repeal Bill: Invasion of the Parliamentary Control Snatchers', EU Law analysis blog, 31 March 2017

49 See Department for Exiting the EU, The exchange and protection of personal data - a future partnership paper, 24 August 2017.

be required in practice to ensure regulatory equivalence? Implementing the GDPR will not be enough on its own to ensure a positive data adequacy finding for the UK.[50]

[50] See Elif Mendos Kuşkonmaz, 'Brexit and Data Protection: The Tale of the Data Protection Bill and UK-EU Data Transfers', EU Law Analysis blog, 26 September 2017; Tech UK 'European Union (Withdrawal) Bill Second Reading Briefing', September 2017

3. The Data Protection Bill [HL] 2017-19

In February 2017, Matt Hancock said that GDPR was a "good piece of legislation" and that "signing up" to it was an "important part" of helping to secure the unhindered flow of data between the UK and the EU after Brexit.[51]

The *Data Protection Bill [HL] 2017-19* was introduced on 13 September 2017. The Bill will bring the GDPR and PCJ Directive into UK law. It will repeal the *Data Protection Act 1998*.

The Government has published a range of material on the Bill including Explanatory Notes, an Impact Assessment, and a number of factsheets:

- Bill overview
- General Data Processing
- Law enforcement processing
- National security data processing
- The Information Commissioner and Enforcement

According to the Government, the Bill will "ensure that the UK is prepared for the future after we have left the EU".[52]

However, some commentators have warned that the Bill is not a "panacea" for securing the uninterrupted flow of data after Brexit and that the UK may face challenges in securing an adequacy decision.[53]

---

51 Matt Hancock (Minister for Digital) oral evidence to the Select Committee on the European Union Home Affairs Sub-Committee, 1 February 2017, p1

52 DCMS, *Data Protection Bill Factsheet – Overview*, September 2017, p1

53 Elif Mendos Kuşkonmaz, 'Brexit and Data Protection: The Tale of the Data Protection Bill and UK-EU Data Transfers', EU Law Analysis blog, 26 September 2017

BRIEFING PAPER
Number 7838
10 October 2017

About the Library

The House of Commons Library research service provides MPs and their staff with the impartial briefing and evidence base they need to do their work in scrutinising Government, proposing legislation, and supporting constituents.

As well as providing MPs with a confidential service we publish open briefing papers, which are available on the Parliament website.

Every effort is made to ensure that the information contained in these publicly available research briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Authors are available to discuss the content of this briefing only with Members and their staff.

If you have any general questions about the work of the House of Commons you can email hcenquiries@parliament.uk.

Disclaimer