HOUSE OF COMMONS LIBRARY

BRIEFING PAPER

Number 7838, 22 June 2017

Brexit and data protection

By John Woodhouse

Contents:

Contents

Summary

The basis of EU data protection law is the 1995 Data Protection Directive (95/46/EC), which was implemented into UK law by the *Data Protection Act 1998*. This general Data Protection Directive has been complemented by other legal instruments, such as the e-Privacy Directive for the communications sector. There are also specific rules for the protection of personal data in police and judicial cooperation in criminal matters (Framework Decision 2008/977/JHA).

Since 1995 technological progress and globalisation have profoundly changed the way data is collected, accessed and used. In addition, EU 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; Reg 2016/679)

  This came into force on 24 May 2016. There is two-year transition period for implementation, meaning that the UK is not obligated to apply it until 25 May 2018.

- The **Directive on data transfers for policing and judicial purposes** (2016/680/EU).

  This came into force on 5 May 2016. EU Member States are required to transpose it into their national law by 6 May 2018. The Directive aims to protect citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities and will especially protect the personal data of victims, witnesses and suspects of crime. It will apply to data transfers across borders within the EU as well as, for the first time, setting minimum standards for data processing for policing purposes within each Member State.

The GDPR

The GDPR has attracted more attention than the Directive. It includes new provisions on:

- Increased territorial scope (extra-territorial applicability)
- Penalties
- Consent
- "Privacy by design"
- Data protection officers

It enhances data subjects' rights with new provisions covering:

- Breach notification
- The right to access
- The right "to be forgotten"

A European Commission factsheet (May 2017) gives an overview of the GDPR and what it will mean for citizens and businesses.

The UK and the GDPR

The Government has said that the GDPR will apply in the UK from 25 May 2018.

In February 2017, Matt Hancock, Minister for Digital and Culture, told the Lords Committee on the European Union that the GDPR was a "good piece of legislation". He

said that parts of the *Data Protection Act 1998* would need to be repealed for data processing to be within the scope of the GDPR and that it was "necessary to ensure that we do not end up with the Data Protection Act duplicating or creating inconsistencies with the GDPR, because the GDPR will be directly applicable".

Queen's Speech, June 2017

The Queen's Speech of 21 June 2017 said that a "new law will ensure that the United Kingdom retains its world-class regime protecting personal data". Background briefing notes on the Queen's Speech explain that the Bill would:

- ensure that our data protection framework is suitable for our new digital age, and cement the UK's position at the forefront of technological innovation, international data sharing and protection of personal data;
- strengthen rights and empower individuals to have more control over their personal data including a right to be forgotten when individuals no longer want their data to be processed, provided that there are no legitimate grounds for retaining it;
- establish a new data protection regime for non-law enforcement data processing, replacing the Data Protection Act 1998; and
- modernise and update the regime for data processing by law enforcement agencies

What will happen after Brexit?

Under the EU's data protection framework, any country outside the EU and EEA 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).

In a February 2017 speech, Elizabeth Denham, the Information Commissioner, said the "big question" was what would happen after the UK leaves the EU. The Government has stressed that it is "keen to secure the unhindered flow of data between the UK and the EU post-Brexit". However concerns have been expressed as to whether the UK's domestic data protection regime will be considered "adequate". This matter was looked at in some detail earlier this year by the Lords Select Committee on the European Union.

1. Background

The right to the protection of personal data is explicitly recognised by Article 8 of the European Union's Charter of Fundamental Rights and by the Lisbon Treaty. The Treaty provides a legal basis for rules on data protection for all activities within the scope of EU law under Article 16 of the Treaty on the Functioning of the European Union.

The basis of EU data protection law is the 1995 Data Protection Directive (95/46/EC), which was implemented into UK law by the *Data Protection Act 1998*. This general Data Protection Directive has been complemented by other legal instruments, such as the e-Privacy Directive for the communications sector. There are also specific rules for the protection of personal data in police and judicial cooperation in criminal matters (Framework Decision 2008/977/JHA).

Since 1995 technological progress and globalisation have profoundly changed the way data is collected, accessed and used. In addition, EU 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. The framework consisted of two documents: a draft Regulation legislating for general data protection across the EU and a draft Directive with the specific aim of protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities. The draft Regulation would repeal and replace the 1995 Directive. The draft Directive would repeal and replace the existing Data Protection Framework Decision of 2008.[1]

This Paper concentrates on the resultant General Data Protection Regulation (GDPR). The GDPR has attracted the most attention so far – for example, on what it means for citizens and businesses, and what will happen after the UK leaves the EU.

[1] For the earlier history see the Library Briefing Paper, *The draft EU Data Protection Framework*, June 2013

2. The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR; Reg 2016/679) was finally agreed by the European Parliament in April 2016 after more than four years of deliberations. It came into force on 24 May 2016. There is a two-year transition period for implementation, meaning that the UK is not obligated to apply it until 25 May 2018. As a Regulation, it will have direct application in Member States.

As online platforms are often offering services to users across the EU, there will be an increasing need to address issues of data protection compliance at an EU, rather than national, level. The Regulation is designed to give citizens more control over their own private information. It updates the principles set out in the 1995 Directive to cover, for example, data processed on the internet (for such purposes as social networks, online shopping and e-banking services) and offline (including for hospital and university registers, company registers of clients and personal data held for research purposes). Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location.

2.1 The GDPR's key provisions

The European Council website gives a useful summary of the Regulation's key provisions:

> **Data subject's rights**
>
> It lists the rights of the data subject, that is the individual whose personal data is being processed. These strengthened rights give individuals more control over their personal data, including through:
>
> - the need for the individual's clear consent to the processing of personal data
> - easier access by the subject to his or her personal data
> - the rights to rectification, to erasure and 'to be forgotten'
> - the right to object, including to the use of personal data for the purposes of 'profiling'
> - the right to data portability from one service provider to another
>
> It also lays down the obligation for controllers (those who are responsible for the processing of data) to provide transparent and easily accessible information to data subjects on the processing of their data.
>
> **Compliance**
>
> It details the general obligations of the controllers and of those processing the personal data on their behalf (processors). These include the obligation to implement appropriate security

measures, according to the risk involved in the data processing operations they perform (risk-based approach). Controllers are also required in certain cases to provide notification of personal data breaches. All public authorities and those companies that perform certain risky data processing operations will also need to appoint a data protection officer.

Monitoring and compensation

The regulation confirms the existing obligation for member states to establish an independent supervisory authority at national level. It also aims to establish mechanisms to create consistency in the application of data protection law across the EU. In particular, in important cross-border cases where several national supervisory authorities are involved, a single supervisory decision is taken. This principle, known as the one stop shop, means that a company with subsidiaries in several member states will only have to deal with the data protection authority in the member state of its main establishment.

The agreement includes the setting up of a European Data Protection Board. This board would consist of representatives of all 28 independent supervisory authorities and would replace the existing Article 29 Committee.

It recognises the right of data subjects to lodge a complaint with a supervisory authority, as well as their right to judicial remedy, compensation and liability. To ensure proximity for individuals in the decisions that affect them, data subjects will have the right to have a decision of their data protection authority reviewed by their national court. This is irrespective of the member state in which the data controller concerned is established.

It provides for very severe sanctions against controllers or processors who violate data protection rules. Data controllers can face fines of up to €20 million or 4% of their global annual turnover. These administrative sanctions will be imposed by the national data protection authorities.

Transfers to a third country

It also covers the transfer of personal data to third countries and international organisations. To this end, it puts the Commission in charge of assessing the level of protection given by a territory or processing sector in a third country. Where the Commission has not taken an adequacy decision on a territory or sector, transfer of personal data may still take place in particular cases or when there are appropriate safeguards (standard data protection clauses, binding corporate rules, contractual clauses).[2]

A European Commission factsheet (May 2017) also gives an overview of the GDPR and how it will benefit citizens and businesses. A dedicated EU GDPR portal is designed "to educate the public about the main elements" of the Regulation.

The Open Rights Group has said that "the final version of the regulation is a mixed bag of results from a civil society perspective".[3]

---

2 Europa website: Data protection reform – the general data protection regulation [accessed 21 June 2017]

3 Open Rights Group blog, "Data Privacy Day: the new EU Data Protection Regulation explained", 28 January 2016. The Group describes itself as "the UK's only digital campaigning organisation working to protect the rights to privacy and free speech online"

2.2 The UK and the GDPR

The Government has said that the GDPR will apply in the UK from 25 May 2018.[4]

In February 2017, Matt Hancock, Minister for Digital and Culture[5], told the Lords Select Committee on the European Union that the GDPR was a "good piece of legislation".[6] The Minister was asked what changes would need to be made to the *Data Protection Act 1998* to bring it into compliance with the GDPR. Mr Hancock said:

> (…) Parts of the Data Protection Act 1998 will need to be repealed for data processing to be within the scope of the GDPR. It is necessary to ensure that we do not end up with the Data Protection Act duplicating or creating inconsistencies with the GDPR, because the GDPR will be directly applicable. We will bring forward legislation in the next session in order to put that into practice.[7]

In April 2017, the Department for Culture, Media and Sport (DCMS) published a consultation seeking views on derogations from the GDPR. The consultation closed on 10 May 2017. The responses are now being analysed.[8]

Queen's Speech, June 2017

The Queen's Speech of 21 June 2017 said that a "new law will ensure that the United Kingdom retains its world-class regime protecting personal data". Background briefing notes on the Queen's Speech state that the Bill would:

> • ensure that our data protection framework is suitable for our new digital age, and cement the UK's position at the forefront of technological innovation, international data sharing and protection of personal data;
>
> • strengthen rights and empower individuals to have more control over their personal data including a right to be forgotten when individuals no longer want their data to be processed, provided that there are no legitimate grounds for retaining it;
>
> • establish a new data protection regime for non-law enforcement data processing, replacing the Data Protection Act 1998; and
>
> • modernise and update the regime for data processing by law enforcement agencies[9]

---

4 DCMS, *Call for views on the General Data Protection Regulation derogations*, April 2017, p1

5 Responsibility for data protection policy transferred from the Ministry of Justice to the DCMS on 17 September 2015: Prime Minister, Machinery of Government Changes, Written Statement [HCWS209], 17 September 2015

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

7 Ibid, p6

8 Gov.UK, General Data Protection Regulation: Call for Views [accessed 21 June 2017]

9 Prime Minister's Office, Background briefing notes on the Queen's Speech, 21 June 2017, p16

2.3 Implementation and advice

The Information Commissioner's Office has said: "if you are currently subject to the DPA, it is likely that you will also be subject to the GDPR".[10]

The Information Commissioner, Elizabeth Denham, has said that the "impact on businesses depends on how much work they have already done to comply with the current regime":

> We have had the Data Protection Act in the UK since 1998…the GDPR has higher standards, but they are evolved standards. If a company has not been doing anything for the last 10 years on data protection, yes, the resource implications are going to be larger…[11]

In February 2017, the Lords Committee on the European Union asked Matt Hancock about the resource implications of bringing the UK into compliance with the GDPR. He said:

> (…) this will, of course, place some requirements on companies, particularly data-heavy companies, to make sure that they comply. However, my view is that the requirements that it brings in are consistent with best practice for handling data, anyway. 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. I do not think that that is a bad thing, given that data is increasingly important in corporate activity.[12]

The ICO has published general guidance for organisations and businesses. The ICO also has a helpline to answer more specific queries: 0303 123 1113.

The GDPR also has implications for regulators. The European Commission and national data protection authorities (DPAs) will have to provide sufficient resources and power to enforce implementation.

---

10 ICO, *Overview of the General Data Protection Regulation (GDPR)*, June 2017, p5

11 Information Commissioner's oral evidence to the Select Committee on the European Union Home Affairs Sub-Committee, 8 March 2017, pp13-4

12 Matt Hancock (Minister for Digital) oral evidence to the Select Committee on the European Union Home Affairs Sub-Committee, 1 February 2017, p6

3. Data protection after Brexit

In a February 2017 speech, the Information Commissioner said the "big question" was what would happen after the UK leaves the EU:

> (…) The legal relationship answers are for government to give – I'm a regulator, independent of government - but they've made it clear that EU law will remain UK law, until the government sees fit to repeal it.
>
> Of course it's possible that in the years after the UK leaves the EU, Parliament will debate amending the requirements of the GDPR. If that happens, we'll be at the centre of any conversations around this, and will be banging our drum for continued protection and rights for consumers and clear laws for organisations.
>
> The government will also need to answer the question about whether the UK will seek to keep the UK's data protection law at an equivalent standard to the EU, to allow unrestricted data flows with EU countries. We need strong data protection laws to achieve all that…[13]

In March 2017, the Lords Select Committee on the European Union was told that after leaving the EU "the critical consideration will be the extent to which the UK is perceived to be adequate, from the EU's perspective, for data protection".[14]

Some business leaders and lawyers have expressed concern at what will happen after Brexit.[15]

The Government has stressed that it is "keen to secure the unhindered flow of data between the UK and the EU post-Brexit. We think that signing up to the GDPR data protection rules is an important part of helping to deliver that".[16]

"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).

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

---

13 "Elizabeth Denham's speech at the DMA Annual Conference", ICO website, 24 February 2017

14 Oral evidence to the Select Committee on the European Union Home Affairs Sub-Committee, 1 March 2017, Stewart Room on p1

15 See, for example, "Brexit: Business and security risks of leaving EU data sharing scheme 'not on Tories' radar', experts warn", *Independent*, 3 June 2017

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

3.1 The UK as a "third country"?

In February and March 2017, the House of Lords Select Committee on the European Union took evidence from the DCMS, the Information Commissioner and a number of academics and lawyers on what would happen after the UK leaves the EU and whether it would be treated as a "third country".

The Government's view

Matt Hancock, Minister of State for Digital and Culture, was asked what would happen if the UK had not secured an adequacy decision:

> (…) once we are no longer in the EU, what will be the default position, as a matter of law, for data flows between the UK and the EU if we have not secured an adequacy decision at the point at which we leave? Secondly—this follows naturally from the previous question - will we seek an adequacy decision as part of the negotiations on Brexit? I know that you are not allowed to say much about that.

The Minister replied:

> (…) We are keen to ensure that data flows are unhindered. As you have anticipated, I will not go into the details of how we do that when negotiations are yet to begin. Our goals are clear. We want an arrangement that provides for the unhindered exchange of data, within an appropriate data protection environment. However, I do not think that it is appropriate to speculate on what arrangements we may seek to put in place.
>
> (…) 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, it is very important that our data rules work, so that there is an uninterrupted system in place.[17]

When asked about an adequacy decision, Matt Hancock said:

> An adequacy decision could work. There are many different ways in which you could make this work. 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.[18]

When pressed on what the default position would be if an adequacy decision wasn't secured, he replied: "We are seeking to have unhindered data flows. We are confident of being able to achieve that". He did not go through any options in case this "fetter[ed]" discussion in future negotiations.[19]

---

17 Matt Hancock (Minister of State for Digital and Culture) oral evidence to the Select Committee on the European Union Home Affairs Sub-Committee, 1 February 2017, p3

18 Ibid, pp4-5

19 Ibid, p5

The Information Commissioner's view

The Information Commissioner was asked what the "default position" would be if the UK failed to secure an "equivalence deal" with the EU. She replied:

> I have said publicly and to the Government that, in my view, the best way forward is to achieve an adequacy finding from the European Commission. That is the best way forward because it is the most straightforward arrangement for the commercial sector and certainly for citizens and consumers who want their data transferred and interchanged between the EU and the UK. We want data flows to continue; it is the most straightforward process by which to achieve that.
>
> Achieving adequacy on day one after exiting the EU may be challenging, because there is a legal process involved, which includes assessment and obtaining an opinion from the Article 29 working party, which is all my counterparts working together in the EU. It is up to government. 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 everybody.[20]

When asked what would happen if it proved impossible to reach an agreement on the continuing flow of data, the Commissioner said:

> Again, it is not for me as the regulator to determine what the regulatory measures and environment will look like after exit. However, there are measures other than adequacy that allow data to continue flowing. In the general data protection regulation, similar to the existing law today, 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.[21]

The Commissioner also made the following observation on alternatives to an adequacy decision:

> There are only, I believe, nine jurisdictions that have an adequacy finding, or at least a partial finding, by the [European] Commission. Canada is one of those jurisdictions, but it is a partial adequacy finding just for the commercial sector…
>
> I would like to make one more point about that. Comparing the UK to other countries that do not have adequacy is missing a major point. There is 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 arrangement and be just like - you can pick a country - Turkey or Argentina. It is just not the same…[22]

In a separate evidence session to the Committee, a number of academics and lawyers were asked about data protection after Brexit. Stewart Room (global head of cybersecurity and data protection legal services at PricewaterhouseCoopers) said that adequacy decisions had benefits over other options:

---

20 Information Commissioner's oral evidence to the Select Committee on the European Union Home Affairs Sub-Committee, 8 March 2017, p4
21 Ibid, p5
22 Ibid, p6

> (…) Multinational businesses want to build to a common standard. They want certainty. They want to build their technology systems, digital environments and cyber positions to a single common standard. An adequacy decision gives certainty to businesses and to the economy that the United Kingdom's law is accepted as being of the right nature and having the right properties…[23]

He also said that the development of an adequacy decision could take "many, many years".[24]

The Committee asked Rosemary Jay (a lawyer and academic on data protection) how "straightforward" it would be to negotiate an agreement with the EU:

> Lord O'Neill of Clackmannan: …At the moment, one would imagine that the UK's standards are on all fours with the 27. Would that enable us to arrive at a point-of-departure arrangement, which would allow us to keep abreast of changes within the EU in the future?

Rosemary Jay said:

> (…) 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. At the moment, it has to go to the Article 31 Committee and then the Article 29 Committee; then the Commission has to make its decision. 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.[25]

Stewart Room pointed out that in negotiations there would be a shared interest in maintaining strong data protection:

> The issue about the ability to conduct a negotiation has to be seen in the context of all the issues and which are perceived to be priorities. I sense a slight difference between the topic of data protection and some of the other topics that would need to be addressed, such as trade barriers. 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…[26]

---

23 Oral evidence to the Select Committee on the European Union Home Affairs Sub-Committee, 1 March 2017, Stewart Room on p7
24 Ibid, p4
25 Ibid, p8
26 Ibid, p8

Valsamis Mitsilegas (Professor of European Criminal Law at QMUL) said:

> (…) [On] where we go now, adequacy will be seen in terms of domestic UK law. While in the case of private law and the data protection regulation it is very likely that we will see a level playing field, 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. That will not be as easy in this context.[27]

[27] Ibid, p9

BRIEFING PAPER
Number 7838
22 June 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