HOUSE OF COMMONS LIBRARY

**BRIEFING PAPER**

Number 7838, 15 December 2016

# Brexit and data protection

By Philip Ward

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 is now in force, but there is a 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 is now in force and EU Member States are required to transpose it into their national law by May 2018.

The Regulation has attracted far more attention than the Directive. The Regulation includes new provisions covering

- 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"

On present estimates it is unlikely that the UK will have left the European Union by May 2018. The GDPR will therefore apply from that date until "Brexit" occurs and UK businesses are being advised to prepare accordingly. There is a dedicated EU GDPR portal and general guidance is available on the Information Commissioner's website.

Concerns have been expressed as to what will happen after "Brexit", particularly whether the UK's domestic data protection regime will be considered "adequate" by the EU and whether recent UK legislation is compatible with the GDPR. The Government has said that it is working "to make sure that we achieve a coherent data protection regime and that data flows with the EU are not interrupted after we leave".

# 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 Regulation, which has attracted the most attention.

[1] This has been a long time in the making. For the earlier history see Library Briefing Paper 6669, *The draft EU Data Protection Framework*, June 2013

# 2. The 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. 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. There is a dedicated EU GDPR portal and general guidance for organisations and businesses on the Information Commissioner's website. The Commissioner's Office (ICO) also has a helpline to answer more specific queries: 0303 123 1113.

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.

The European Council provides this 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'[2]
- 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.

[2] This "right to erasure" is similar to one that already exists (see our Library Paper on *The "right to be forgotten"*, September 2014). The earlier right derives from a European Court of Justice ruling on the 1995 Directive,

## 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).[3]

The GDPR applies to "controllers" and "processors". The definitions are broadly the same as under the UK's current *Data Protection Act 1998* (DPA) – i.e. the controller says how and why personal data is processed and the processor acts on the controller's behalf. The ICO's advice is that "if you are currently subject to the DPA, it is likely that you will also be subject to the GDPR".

The Regulation enshrines the principle of "privacy by design" by calling for the inclusion of data protection from the onset of the designing of systems, rather than an addition. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

One of the reports which made up the *Review of the Balance of Competences* commissioned by the last Government was devoted to 'Information Rights'. Respondents identified the proposed EU Regulation as a key opportunity and challenge for the future. While some respondents welcomed the Commission's action in this area, they queried whether the proposed provisions struck the correct balance in protecting individuals. Many highlighted the instrument's prescriptive nature, which in their view threatens to have a negative impact on several business sectors. The report identified four broad themes:

> (i) The need to be aware of interaction between principles of data protection and access to information;
>
> (ii) The need to make sure any legislation is future proofed, given the potential for further unpredictable changes in data use;
>
> (iii) The need to find a balance between an approach towards greater common standards, and sufficient flexibility for different sectors, and the different circumstances in Member States;
>
> (iv) The need for greater understanding and engagement with stakeholders in this complex, diverse, and rapidly-changing field.[4]

At earlier stages in the evolution of this Regulation, the then (Coalition) Government expressed reservations. The concern was to negotiate an instrument that did not overburden business, the public sector or other organisations, and that encouraged economic growth and innovation, at the same time as ensuring that people's personal data is protected.[5] In summer 2015, Dominic Raab, then a Minister, said in a Written Statement to the House:

> My Noble Friend the Minister of State for Civil Justice (Lords Minister), Lord Faulks QC, attended the Justice and Home Affairs Council on the 16 June, where a General Approach was agreed on the General Data Protection Regulation. Notwithstanding

---

3 For another useful summary, see *Communications Law* 21(2), 2016, p8. For greater detail see the ICO's guidance and Allen & Overy, *The General Data Protection Regulation*, 2016

4 HM Government, *Review of the Balance of Competences between the United Kingdom and the European Union: Information Rights*, December 2014, pp6-7

5 See section 4 of Library Briefing Paper 6669, *The draft EU Data Protection Framework*, June 2013

> serious concerns, the UK voted in favour of the General Approach, with a view to mitigating the negative implications of the text during the subsequent trilogue discussion, and without prejudice to our decision on the final outcome of negotiations…My Noble Friend the Minister of State for Civil Justice (Lords Minister), Lord Faulks QC, attended the Justice and Home Affairs Council on the 16 June, where a General Approach was agreed on the General Data Protection Regulation. Notwithstanding serious concerns, the UK voted in favour of the General Approach, with a view to mitigating the negative implications of the text during the subsequent trilogue discussion, and without prejudice to our decision on the final outcome of negotiations.[6]

Organisations that will be caught by new requirements have expressed a range of views.[7] The Open Rights Group concludes that "the final version of the regulation is a mixed bag of results from a civil society perspective".[8] The implementation of the GDPR will require comprehensive changes of business practices for companies that had not implemented a comparable level of privacy before the Regulation entered into force (especially non-European companies handling EU personal data). There are also implications for regulators. The European Commission and national data protection authorities (DPAs) will have to provide sufficient resources and power to enforce the implementation and a unique level of data protection has to be agreed upon by all European DPAs, since a different interpretation of the Regulation might still lead to different levels of privacy.

---

6 [Scrutiny override on the data protection regulation] - HCWS126, 26 July 2015

7 These are summarised in the Wikipedia article on the GDPR. More opinion from IT professionals in: "Brexit will happen. The EU GDPR will happen. You can't avoid either", *The Register*, 16 September 2016

8 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".

# 3. The Directive

The new data protection regime also includes a Directive on data transfers for policing and judicial purposes.[9] This is now in force and EU Member States are required to transpose it into their national law by 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.

9 2016/680/EU

# 4. What will happen after Brexit?

It seems unlikely, on present estimates, that the UK will have left the EU by May 2018. The GDPR will therefore apply from that date until "Brexit" occurs.

The Government has been pressed on this issue – for example, when the Culture Secretary, Karen Bradley, appeared before the Culture, Media and Sport Committee on 24 October 2016.[10] In her evidence Ms Bradley indicated that organisations can expect the GDPR to apply directly in the UK, at least for a time, despite the UK's move towards Brexit. She said:

> Q72…We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public.

In a Written Statement on 7 November 2016 announcing the publication of the Triennial Review of the Information Commissioner's Office, the Minister, Matt Hancock, said:

> …The new Information Commissioner, Elizabeth Denham, took up post in July 2016. Her first priority is to ensure that the organisation is properly equipped to take forward the requirements of the General Data Protection Regulation (GDPR), which will come into force in the UK in May 2018; and to provide clarity and certainty to businesses and organisations as they make preparations to implement the Regulation. Alongside this is a need to prepare the organisation for any changes to data protection regulatory landscape after the UK exits the European Union. (HCWS238)

As to what happens after that, legal commentators have written:

> Once outside the EU, if the UK leaves in place the DPA, or replaces it with a light version of the GDPR, there is a risk that the European Commission would not regard the UK as a "safe third country" (one that has "adequate protection" of citizens' rights) for the receipt of the personal data of EU citizens. There would need to be a Safe Harbour data transfer pact at EU/UK level, or binding Corporate Rules or the use of Model Clause Agreements at an organisational level.[11]

Given that the GDPR also applies to organisations outside the EU that offer goods or services to EU citizens, this suggests that, post-Brexit, UK organisations wishing to trade with the EU will still need to comply with the GDPR.

In an adjournment debate on 12 December 2016, Daniel Zeichner foresaw problems ahead for data transfer:

> There is a risk that after Brexit the UK may be treated as a "third country" on data protection issues. (…) In a perhaps exquisite irony, we would find our legislation being judged against the

[10] Data protection policy is now a responsibility of the Department for Culture, Media and Sport, having previously sat with the Ministry of Justice.

[11] "Brexit – the impact on media law", *Entertainment Law Review* 27(7), 2016, 229-32

> standards of the GDPR. We would be a third country and could be required to come to what is termed an "adequacy decision" with the EU to allow data to flow freely between the United Kingdom and EU member states and to enable trade with the single market on equal terms.
>
> In order to adopt an adequacy decision, the European Commission must be satisfied that a third country offers an equivalent level of data protection. A number of commentators fear that the recent Investigatory Powers Act means that the Commission may take some convincing. The risk is that such negotiations could take years to resolve, leaving protections for UK citizens in the meantime weak, as well as hugely disadvantaging the crucial tech sector, one of our great success stories…[12]

In reply, the Minister, Matt Hancock, said the matter was in hand:

> We have made progress in our argument within the EU that data localisation rules are not appropriate. That is a live issue in the EU at the moment. There is also work to be done between now and 2018 to make sure that we achieve a coherent data protection regime and that data flows with the EU are not interrupted after we leave. The Government are considering all options for the most beneficial way of ensuring that the UK's data protection regime continues to build a culture of data confidence and trust that safeguards citizens and supports businesses in a global data economy.[13]

There has also been intermittent discussion of the GDPR during the passage of the *Digital Economy Bill*. For example, in Committee, the Opposition questioned how the Bill's elements conform with the GDPR. The GDPR includes stronger provisions than existing UK law on processing only the minimum data needed, consent, requirements on clear privacy notices, explicit requirements for data protection by design and by default, and on carrying out data protection impact assessments. Louise Haigh (Lab) was unclear how data sharing as provided for under the Bill would comply with the GDPR obligations on informed consent and the ability to revoke consent.[14] When a similar point was raised by Daniel Zeichner in his adjournment debate, the Minister explained that

> The Bill is drafted according to the current law, which is the Data Protection Act. It is not possible to draft legislation in anticipation of future legislation; that is not how the body of legislation works. If and when legislation is proposed to amend an existing system such as the Data Protection Act, one would expect it to include an amendment to the Digital Economy Bill, should this Parliament enact it, in order to make it consistent.[15]

In outlining its plans for Brexit, the Government has said that it will introduce a "*Great Repeal Bill*". The Bill, once given effect, will remove the *European Communities Act 1972* from the UK statute book and enshrine any EU laws in effect into UK law.[16] Withdrawal from the EU

---

12 HC Deb 12 December 2016 c591
13 HC Deb 12 December 2016 c594
14 For summary of debates, see the Library's *Committee Stage Report on the Digital Economy Bill*, November 2016, pp34 and 37-8
15 HC Deb 12 December 2016 cc594-5
16 See Library Briefing Paper 7793, *Legislating for Brexit: the Great Repeal Bill*

would mean that UK rights currently guaranteed by EU law would no longer be so guaranteed. In consequence, a post-Brexit government could seek to amend or remove any of these.

In a speech on 29 September 2016, the Information Commissioner, Elizabeth Denham, said that it was likely that the GDPR would apply in the UK before the UK leaves the EU. She said, however, that if that is not the case or if the UK Government decides to apply alternative rules to those in the GDPR post-Brexit, the UK rules would "still need to be deemed adequate or essentially equivalent" to the GDPR to preserve data flows between Europe and the UK. Ms Denham said that future UK data protection laws after Brexit "should be developed on an evolutionary basis, to provide a degree of stability and clear regulatory messages for data controllers and the public".

In one passage of her speech headed "Brexit and the GDPR", Ms Denham (with a nod to Donald Rumsfeld) set out the "known knowns" and the "known unknowns" of the post-Brexit future:

> …Let's start with the known knowns. It is extremely likely that GDPR will be live before the UK leaves the European Union. Remember that the GDPR is actually already in force, it is just that Member States are not obligated to apply it until 25 May 2018.
>
> The digital world is a smaller world. Copenhagen consumers are closer, Sofia's citizens aren't so far away. For most people in this room, the GDPR will be something you'll have to follow, to do business where you want to.
>
> GDPR brings in new elements – and a more 21st century approach – the right of consumers to data portability is new, as is mandatory data breach reporting, higher standards of consent, and significantly larger fines for when companies get things wrong. But the major shift in the law is about giving consumers control over their data. It ties in with building trust and is also part of the ICO's philosophy.
>
> We are helping you to get ready for the new law – and we will continue to provide advice and guidance around GDPR, whether you're a business with 400 customers or 40 million.
>
> What about the known unknown territory? That's those of you who only operate in the UK. We know it's up to government what happens here, both in that middle period from May 2018 to whenever the UK formally leaves the EU, and beyond.
>
> The fact is, no matter what the future legal relationship between the UK and Europe, personal information will need to flow. It is fundamental to the digital economy. In a global economy we need consistency of law and standards – the GDPR is a strong law, and once we are out of Europe, we will still need to be deemed adequate or essentially equivalent. For those of you who are not lawyers out there, this means there would be a legal basis for data to flow between Europe and the UK.
>
> The adequacy issue is one I've experienced first-hand. The impact of the demise of Safe Harbor, the data sharing agreement between the EU and the US, had repercussions outside of the US. In Canada many were questioning whether the European Union Court of Justice's threshold for privacy could call our own adequacy into question. I understand this arena. We're talking

about proper protection for consumers, about certainty for business, and about strong independent oversight of the law.

We'd all like a concrete answer about the specific outlines of post Brexit data protection law. We know businesses don't generally like uncertainty. But in the end, it's government that will have to decide.

Legislative change does bring nervousness, but it also brings opportunity. These changes – stronger data protection law and enforcement – are aimed at inspiring public trust and confidence. GDPR is an incentive to improve your practices, to sharpen things up, and encourage organisations to look at things afresh…

**BRIEFING PAPER**
Number 7838
15 December 2016

## 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