HOUSE OF LORDS Library Briefing

Data Protection Bill [HL] (HL Bill 66 of 2017–19)

Summary

The Data Protection Bill [HL] was introduced in the House of Lords by Lord Ashton of Hyde, Parliamentary Under Secretary at the Department for Digital, Culture, Media and Sport (DCMS), on 13 September 2017, and is scheduled to receive its second reading on 10 October 2017. DCMS has published detailed Explanatory Notes to the Bill and a range of factsheets and other documentation on various aspects of the Bill. This briefing should be read in conjunction with this material.

The Bill aims to update the UK's data protection regime, including relevant definitions used in that regime, in accordance with new rules agreed at a European level. In order to do this, it would repeal and replace the Data Protection Act 1998, which provides the basis for the UK's existing data protection framework. The Bill is formed of seven parts—comprising 194 clauses—and 18 schedules, and provides for four main matters: data processing; law enforcement data processing; data processing for national security purposes; and regulatory oversight and enforcement.

Concerning data processing, the Government envisages that the Bill, once implemented, would supplement the EU General Data Protection Regulation due to come into force in May 2018, and continue to do so once that instrument is brought into the corpus of UK law under provisions in the European Union (Withdrawal) Bill currently before Parliament. Regarding law enforcement data processing, the Bill would implement the EU Law Enforcement Directive ahead of the deadline for transposition in May 2018. In relation to data processing for national security purposes, the Bill would transpose principles set out in an updated Council of Europe convention on the processing of personal data (known as the "modernised Convention 108"), which the Government expects to be agreed in due course. Lastly, the Bill would also update the enforcement powers available to the Information Commissioner, as the responsible regulator, and would introduce new offences relating to the processing of personal data, amongst other measures.

The Bill has been welcomed by the Labour Party, Liberal Democrats, the Information Commissioner and other stakeholders, such as the Confederation of British Industry, which represents businesses that would be affected by provisions in the Bill.

Table of Contents

Thomas Brown
5 October 2017

Table of Contents

---

1. Background to the Bill

1.1 Legislative Context

Historical Background

The Council of Europe (CoE) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) opened for signature in 1981.[1] The Convention was the first binding international instrument relating to personal data protection rights and regulating the cross-border flow of personal data. The Convention contained a set of principles to govern data processing, and enshrined the right of an individual to know what information was stored on him or her, subject to possible exemptions relating to national security and/or defence, and, if necessary, to have incorrect records amended.[2]

In 1984, Parliament passed the UK's first Data Protection Act, which incorporated eight data protection principles arising from Convention 108, including that personal data should be obtained and processed fairly and lawfully and that such data should not be held for longer than necessary.[3] The UK ratified Convention 108 in 1985. The 1984 Act, incorporating principles established under Convention 108, provided the UK's data protection framework until the passing of the Data Protection Act 1998.

Data Protection Act 1998

The Data Protection Act 1998, which came into force on 1 March 2000, repealed the Data Protection Act 1984 and provides the legal framework for the UK's existing data protection regime. The Act implemented the EU's 1995 Data Protection Directive, which focused on protecting the right to privacy in respect of the processing of personal data and on ensuring the free flow of personal data between EU member states—with minimal divergence across jurisdictions. The scope of the 1998 Act is wider than the 1995 Directive as it covers all general data processing, including for national security purposes (with certain exemptions).[4]

European Union: General Data Protection Regulation and Law Enforcement Directive

In January 2012, the European Commission proposed reform of data

---

[1] Council of Europe, 'Details of Treaty No. 108', accessed 22 September 2017.

[2] Explanatory Notes, p 17; and Council of Europe, 'Details of Treaty No. 108', accessed 22 September 2017. For further information on the Convention, see Council of Europe, *Explanatory Report to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 28 January 1981.

[3] Explanatory Notes, p 17; and Data Protection Act 1984.

[4] Explanatory Notes, p 18.

protection rules across the EU.[5] Four years later, in April 2016, the General Data Protection Regulation (GDPR) and Law Enforcement Directive (LED) were adopted by the European Council and European Parliament.[6] The Commission has stated that the objective of the new set of rules is to "give citizens back control over their personal data, and to simplify the regulatory environment for business".[7] Regarding the latter, the Commission has estimated that the reduction in fragmentation and administrative burdens following the application of the new rules would lead to savings of around €2.3 billion a year for businesses.[8]

Part 2 of the Bill implements the GDPR standards across all general data processing; defines terms used in the Regulation in the UK context; and exercises several available derogations within the GDPR.[9] The Regulation replaces the 1995 Data Protection Directive and broadens the definition of 'personal data' to include categories of data such as IP addresses and internet cookies. It also widens special categories to include genetic and biometric data where these data would be used to uniquely identify an individual.[10] The GDPR strengthens some of the rights carried over from the Data Protection Act 1998, including in respect of a right to erasure so that an individual could request the deletion of data when they withdraw consent or when that data was processed for the purposes of providing a service to a child (for example, by a social media company).[11] The Regulation will apply from 25 May 2018.[12]

EU regulations are directly applicable to member states under the Treaty on the Functioning of the European Union. The Government has indicated that primary legislation is required to supplement the Directive, until the instrument is brought into UK law in line with provisions in the European Union (Withdrawal) Bill, because there are derogations (exemptions) within the GDPR where the UK wishes to exercise discretion over how certain provisions would apply. The Government has described these possible

---

[5] European Commission, 'Reform of EU Data Protection Rules', accessed 25 September 2017.

[6] ibid. The Law Enforcement Directive (LED) is also referred to as the Police and Criminal Justice Directive.

[7] European Commission, 'Protection of Personal Data', accessed 25 September 2017.

[8] European Commission, 'Reform of EU Data Protection Rules', accessed 25 September 2017.

[9] Department for Digital, Culture, Media and Sport, *Data Protection Bill Factsheet: Overview*, 14 September 2017, p 2; and Explanatory Notes, p 12. For information on intended exemptions, see in particular schedules 2–4.

[10] Explanatory Notes, p 8.

[11] ibid, p 10–12.

[12] European Commission, 'Protection of Personal Data', accessed 25 September 2017. Text of the Regulation: *Regulation (EU) 2016/679 of the European Parliament and of the Council 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)*, 27 April 2016.

exemptions as "flexibilities permitted within the GDPR".[13] The text the Bill does not reproduce the text of the GDPR, but rather cross refers to the Regulation.[14] The Government has explained that under a European Court of Justice ruling, EU member states are prevented from duplicating the provisions of EU regulations in domestic law.[15]

Part 3 of the Bill provides for a bespoke regime for the processing of personal data by the police, prosecutors and other criminal justice agencies for law enforcement purposes, in line with the LED, which concerns the cross-border processing of personal data by competent authorities for law enforcement purposes and the free movement of such data.[16] Such 'competent authorities' include those public authorities (or bodies entrusted to exercise public authority) competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including those relating to public security.[17] The Directive updates and replaces the 2008 Framework Decision for the police and criminal justice sector, which was transposed into UK law via part 4 of the Criminal Justice and Data Protection (Protocol No 36) Regulations 2014 (SI 2014/3141).[18]

The Bill transposes the provisions of the LED into UK law, whilst also applying these provisions to the domestic processing of personal data for law enforcement purposes. The Government has stated that this approach will ensure that there is a "single domestic and trans-national regime for the processing of personal data for law enforcement purposes across the whole of the law enforcement sector".[19] EU member states are required to transpose the LED into national law by 6 May 2018.[20] It is envisaged that the GDPR will apply to the processing of personal data across the law enforcement sector for purposes other than those relating to law enforcement.

The Government has observed that the House of Commons European Scrutiny Committee and the House of Lords European Union Committee

---

[13] Department for Culture, Media and Sport, *Call for Views on the General Data Protection Regulation Derogations*, 12 April 2017, p 1.
[14] Explanatory Notes, p 18.
[15] Case 39/72 Commission v Italy [1973] ECR 101; Explanatory Notes, p 18.
[16] Department for Digital, Culture, Media and Sport, *Data Protection Bill Factsheet: Overview*, 14 September 2017, p 3; and Explanatory Notes, p 15.
[17] Explanatory Notes, p 15.
[18] ibid, pp 14–5; and European Commission, 'Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market', 15 December 2015.
[19] Explanatory Notes, p 15.
[20] European Commission, 'Protection of Personal Data', accessed 25 September 2017. Text of the Directive: *Directive (EU) 2016/680 of the European Parliament and of the Council 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*, 27 April 2016.

cleared the GDPR and LED from scrutiny in February 2016.[21] In its report, the House of Commons European Scrutiny Committee stated that parliamentary scrutiny of the Data Protection package had been "extensive".[22]

Updated Council of Europe Convention

The CoE is currently in the process of agreeing a modernised Convention on the Protection of Individuals with Regard to the Processing of Personal Data (referred to as 'modernised Convention 108') which includes a number of innovations relating to areas including privacy by design and an obligation to declare data breaches.[23] The CoE has stated that this exercise has two key aims: addressing challenges for privacy resulting from the use of new information and communication technologies; and strengthening the Convention's follow-up mechanism relating to implementation of the Convention.[24]

The Government has implied that the updated Convention is an important mechanism for ensuring that data protection standards are consistent at an international level. The Government has also stated that part 4 of the Bill, relating to the processing of personal data by the intelligence services, is based on the modernised Convention, as data processing in connection with national security issues is not within scope of the GDPR.[25]

1.2 Political and Policy Context

Conservative Party Manifesto

The Conservative Party manifesto published ahead of the most recent general election stated that the Party would, if returned to government, be the "global leader in the regulation of the use of personal data and the internet".[26] It stated that a Conservative government would:

> […] give people new rights to ensure they are in control of their own

---

[21] Explanatory Notes, p 19. See House of Commons European Scrutiny Committee, *Documents Considered by the Committee on 3 February 2016*, 12 February 2016, HC 342-xxi of session 2015–16, p 19; and House of Lords European Union Committee, '*Progress of Scrutiny*', 22 May 2017, EUC-3 of session 2016–17, p 21.

[22] House of Commons European Scrutiny Committee, *Documents Considered by the Committee on 3 February 2016*, 12 February 2016, HC 342-xxi of session 2015–16, p 14.

[23] Explanatory Notes, p 7; and Council of Europe, 'Modernisation of the Data Protection 'Convention 108'', accessed 25 September 2017.

[24] Council of Europe, 'Modernisation of the Data Protection 'Convention 108'', accessed 25 September 2017.

[25] Explanatory Notes, p 16. See also Home Office, *Letter from Minister of State for Security to Chair of the Intelligence and Security Committee*, 19 September 2017.

[26] Conservative Party, *Conservative Party Manifesto 2017*, May 2017, p 38.

> data, including the ability to require major social media platforms to delete information held about them at the age of 18, the ability to access and export personal data, and an expectation that personal data held should be stored in a secure way.[27]

The manifesto added that a Conservative administration would "bring forward a new data protection law, fit for our new data age", to ensure the "very best standards for the safe, flexible and dynamic use of data and enshrining our global leadership in the ethical and proportionate regulation of data".[28]

Queen's Speech 2017

Following the undertakings made in the Conservative manifesto, the Government announced in the June 2017 Queen's Speech that it would bring forward a "new law [to] ensure that the United Kingdom retains its world-class regime protecting personal data".[29] Government briefing notes published alongside the Queen's Speech stated that a Bill would be introduced to establish a data protection regime "fit for the twenty-first century". In the Government's words, 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.
- Modernise and update the regime for data processing by law enforcement agencies.[30]

The briefing notes stated that by enabling effective implementation of the GDPR and LED, the Bill would contribute to the UK meeting its obligations while still a member of the EU and assist in putting the UK in the "best position to maintain our ability to share data with other EU member states and internationally" after the country ceased to be a member of the bloc.[31]

---

[27] Conservative Party, *Conservative Party Manifesto 2017*, May 2017, p 79.
[28] ibid, p 80.
[29] HL *Hansard*, 21 June 2017, col 6.
[30] Prime Minister's Office and Cabinet Office, *Queen's Speech 2017: Background Briefing Notes*, 21 June 2017, p 16.
[31] ibid, p 46.

The Government noted that data protection is a reserved matter, and therefore the Bill would apply to the UK as a whole except for certain clauses which would only extend to one or more domestic jurisdictions.[32]

Consultation and Statement of Intent

Between 12 April and 10 May 2017, the Government ran a consultation on the exemptions to be made under the GDPR including those relating to archiving and research and freedom of expression in the media. This exercise was conducted to "capture views on if and how the Government should implement the defined flexibilities permitted within the GDPR".[33]

There were over 300 responses to the 'call for views', including 155 from individuals and 170 from organisations.[34] The latter consisted of bodies from a range of sectors, including local government entities, businesses, media organisations, heritage institutions and educational and research establishments.[35]

In response, the Government published a statement of intent on 7 August 2017 that set out details of its proposed Data Protection Bill.[36] The document outlined the Government's objectives: maintaining trust and confidence in the data protection regime; retaining the ability to transfer data across international borders and its corresponding importance to the economy and trade; and the ability to collect, share and process personal data for law enforcement and security purposes.[37] It also provided information on the Government's ambitions regarding the various exemptions available under the GDPR, including those relating to consent for the processing of children's personal data online; the processing of criminal conviction and offence data; automated individual decision-making; freedom of expression in the media; and research.[38]

---

[32] Prime Minister's Office and Cabinet Office, *Queen's Speech 2017: Background Briefing Notes*, 21 June 2017, p 46; and Explanatory Notes, p 20 and pp 106–8.
[33] Department for Digital, Culture, Media and Sport, 'General Data Protection Regulation: Call for Views', updated 7 August 2017; and *Call for Views on the General Data Protection Regulation Derogations*, 12 April 2017.
[34] Department for Digital, Culture, Media and Sport, 'General Data Protection Regulation: Call for Views', updated 7 August 2017. The responses are publicly available via this webpage.
[35] Department for Digital, Culture, Media and Sport, *A New Data Protection Bill: Our Planned Reforms—Statement of Intent*, 7 August 2017, pp 25–7.
[36] ibid. Alongside this statement of intent, the Government published a study by London Economics on the benefits arising from personal data rights under the GDPR, including right of access, right to erasure and data portability: London Economics, *Research and Analysis to Quantify the Benefits Arising from Personal Data Rights Under the GDPR*, May 2017.
[37] Department for Digital, Culture, Media and Sport, *A New Data Protection Bill: Our Planned Reforms—Statement of Intent*, 7 August 2017, pp 6–7.
[38] ibid, pp 14–22.

House of Lords European Union Committee Report

On 18 July 2017, following an inquiry by the Home Affairs sub-committee, the House of Lords European Union Committee published a report on the EU data protection package in the context of the UK's withdrawal from the EU.[39] The report supported the Government's stated intention of seeking to maintain the stability of data transfers between EU member states and the UK following Brexit, but stated that the Committee was "struck by the lack of detail on how the Government plans to deliver this outcome". The report continued:

> 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.[40]

The Committee recommended that the Government should pursue and maintain regulatory equivalence with the EU in respect of data protection in order to ensure unhindered data flows between the UK and EU post-Brexit.[41] The report also recommended that the Government should seek an 'adequacy decision' from the European Commission certifying that the UK had equivalent standards and safeguards to allow data to continue to flow freely, the practical effect of which would be that cross-border data transfers could take place without any further safeguards.[42] However, the report noted that such decisions are only taken in respect of third countries and follow a set procedure, which may act as an impediment to uninterrupted equivalence.[43]

The report noted that the alternative to securing an adequacy decision from the Commission would be for individual data controllers and processors to adopt their own safeguards that offered an adequate level of protection to enable personal data to be transferred out of the EU, including "tools such

---

[39] House of Lords European Union Committee, *Brexit: the EU Data Protection Package*, 18 July 2017, HL Paper 7 of session 2017–19.
[40] ibid, p 3.
[41] House of Lords, 'Barrier to Trade and Security if Data Transfers are Hindered After Brexit', 18 July 2017.
[42] House of Lords European Union Committee, *Brexit: the EU Data Protection Package*, 18 July 2017, HL Paper 7 of session 2017–19, p 16.
[43] ibid, p 3; and Barney Thompson, 'UK Lacks Detail on Post-Brexit Data Transfers with EU, Say Lords', *Financial Times (£)*, 18 July 2017. For details of the procedure to be followed in respect of adequacy decisions, and countries and territories recognized as providing adequate protection, see European Commission, 'Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries', accessed 3 October 2017.

as Standard Contractual Clauses, and Binding Corporate Rules".[44] However, the report added that the Committee viewed such arrangements as "less effective than an adequacy decision".

In addition, it has been argued that an agreement would be desirable because the GDPR has extraterritorial applications, meaning that businesses and organisations need to be compliant with the Regulation if they process personal data originating from the EU. This could include, for example, the details provided by an individual based in an EU country when booking a hotel room in the UK.[45]

Government Position Paper

On 24 August 2017, the Department for Exiting the European Union published a government position paper on the exchange and protection of personal data following the UK's departure from the EU.[46] The paper cited an estimate that 75 percent of the UK's cross-border data flows are with EU countries, and set out its ambitions in regard to future cooperation in this area:

> 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.[47]

The document called for an early agreement on mutual recognition of data protection frameworks, and for an "agreed negotiating timeline for longer-term arrangements". Regarding these longer-term arrangements, the position paper also set out the alternatives to adequacy under the GDPR and LED, but reiterated the Government's preference for a UK-EU model

---

[44] House of Lords European Union Committee, *Brexit: the EU Data Protection Package*, 18 July 2017, HL Paper 7 of session 2017–19, p 3.
[45] Tony Greenway, 'GDPR is Coming. Is Your Business Ready for It?', Future of Tech, September 2017.
[46] HM Government, *The Exchange and Protection of Personal Data: A Future Partnership Paper*, 24 August 2017.
[47] ibid, p 2.

for exchanging and protecting personal data that could "build on the existing adequacy model".[48]

2. Overview of the Bill

The Bill comprises seven parts, containing 194 clauses, and 18 schedules. This section briefly outlines the provisions contained within each part of the Bill. The Department for Digital, Culture, Media and Sport (DCMS) has published detailed Explanatory Notes which provide extensive commentary on the individual provisions in the Bill.

The Government has also published a number of factsheets on the Bill, the first of which summarises the main elements of the Bill in brief. This document sets out, under headings, what the Bill aims to do:

General Data Processing

- Implement the GDPR standards across all general data processing.
- Provide clarity on the definitions used in the GDPR in the UK context.
- Ensure that sensitive health, social care and education data can continue to be processed to ensure continued confidentiality in health and safeguarding situations can be maintained.
- Provide appropriate restrictions to rights to access and delete data to allow certain processing currently undertaken to continue where there is a strong public policy justification, including for national security purposes.
- Set the age from which parental consent is not needed to process data online at age 13.

Law Enforcement Processing

- Provide a bespoke regime for the processing of personal data by the police, prosecutors and other criminal justice agencies for law enforcement purposes.
- Allow the unhindered flow of data internationally whilst providing safeguards to protect personal data.

[48] HM Government, *The Exchange and Protection of Personal Data: A Future Partnership Paper*, 24 August 2017, p 8 and pp 11–12; and Mehreen Khan, 'UK Assures on 'Close' EU Data Protection Laws After Brexit', *Financial Times (£)*, 24 August 2017.

National Security Processing

- Ensure that the laws governing the processing of personal data by the intelligence services remain up-to-date and in-line with modernised international standards, including appropriate safeguards with which the intelligence community can continue to tackle existing, new and emerging national security threats.

Regulation and Enforcement

- Enact additional powers for the Information Commissioner who will continue to regulate and enforce data protection laws.
- Allow the Commissioner to levy higher administrative fines on data controllers and processors for the most serious data breaches, up to £17m (€20m) or 4 percent of global turnover for the most serious breaches.
- Empower the Commissioner to bring criminal proceedings against offences where a data controller or processor alters records with intent to prevent disclosure following a subject access request.[49]

2.1 Part 1: Preliminary

Part I comprises clause 1, which provides an overview of the Bill, and clause 2, which defines terms used in the Bill. The Government has stated that the Bill adopts and extends many of the definitions found in the GDPR to apply across the Bill, including the following:

- **Personal Data**: Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **Processing**: 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.

[49] Department for Digital, Culture, Media and Sport, *Data Protection Bill Factsheet: Overview*, 14 September 2017, pp 2–3.

- **Filing System**: Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.[50]

2.2 Part 2: General Processing

Part 2 consists of clauses 3–26 concerning general data processing in line with the GDPR, and includes provision for articles in the GDPR to be taken as if they were part of an Act forming part of UK domestic law. Specifically, this part includes provisions relating to:

- Terms used in the Regulation, including 'controller', 'public authority' and 'public body'.
- The lawfulness of processing, ie that such activity is lawful where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- Special categories of personal data, including that which would reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data and biometric data (where used to identify an individual), and data concerning a person's health, sex life or sexual orientation.
- The rights of data subjects, including in relation to fees, credit reference agencies and automated decision making.
- Restriction on these rights, including exemptions and the power to make further exemptions by regulations.
- Accreditation of certification providers in the context of a compliance mechanism.
- Transfers of personal data to third countries.
- Safeguards for specific processing situations including for archival, research and statistical purposes.[51]

Part 2 also includes provision relating to exemptions for manual unstructured data held by Freedom of Information public authorities or used in longstanding historical research and for national security and defence purposes, subject to certification by a Minister of the Crown.[52]

Schedule 1 to the Bill sets out conditions that must be met when personal data falls into one or more sensitive categories, including employment; health and social care; the prevention and detection of crime; parliamentary, statutory or government purposes; counselling; occupational pensions;

---

[50] Explanatory Notes, p 21.
[51] Explanatory Notes, pp 22–8.
[52] ibid, pp 29–30.

insurance; political matters; and anti-doping in sport.[53] Under part 4 of this schedule, data controllers holding these types of data should have an 'appropriate policy document' that explains the retention and erasure practices in place for the data. It has been noted that these 'additional safeguards' highlight the importance of policy documents and processing records (which have been optional but are now envisaged as mandatory duties) under the GDPR regime.[54]

Schedules 2–4 detail the exemptions, restrictions and derogations the Government has chosen to exercise under the GDPR, which permit departure from particular aspects of that regime, ranging across a large number of areas including crime and taxation; immigration; parliamentary privilege; legal professional privilege; journalism; research and statistics; archiving; educational records; and child abuse data.[55]

Clause 13 relates to the rights of data subjects in respect of automated decision making (processing without human intervention), for example in the case of automated credit checks. Observers, such as Robin Hopkins, a data protection specialist at 11KBW Chambers, have noted that the trend towards such decision making represents a "challenging new area of data protection law".[56] This clause provides that data subjects must be notified 'as soon as reasonably practicable' when such processing takes place, after which the data subject has 21 days in which to object to an automated decision.[57]

Concerns have been raised about clause 15, which would permit alteration of the application of the GDPR by regulations subject to the affirmative resolution procedure, including the amendment or repeal of any of the derogations contained in the Bill.[58] For example, Oliver Butler, a Research Fellow at the University of Oxford, has observed that this power "recalls the controversial clause 152 of the Coroners and Justice Bill 2009" and would represent a "massive shift of control over the legal bases for processing personal data from Parliament to the executive". He called for it not to be passed "without careful scrutiny".[59]

---

[53] Schedule 1; and Robin Hopkins, 'The Data Protection Bill: A Brief Overview', Thomson Reuters Practical Law, 25 September 2017.
[54] Robin Hopkins, 'The Data Protection Bill: A Brief Overview', Thomson Reuters Practical Law, 25 September 2017.
[55] Schedules 2–4; and Robin Hopkins, 'The Data Protection Bill: A Brief Overview', Thomson Reuters Practical Law, 25 September 2017.
[56] Robin Hopkins, 'The Data Protection Bill: A Brief Overview', Thomson Reuters Practical Law, 25 September 2017.
[57] Clause 13.
[58] Explanatory Notes, p 26.
[59] Oliver Butler, 'The Data Protection Bill and Public Authority Powers to Process Personal Data: Resurrecting Clause 152 of the Coroners and Justice Bill 2009?', UK Constitutional Law Association Blog, 28 September 2017.

2.3 Part 3: Law Enforcement Processing

Part 3 is comprised of clauses 27–79, covering data processing for law enforcement purposes. Clauses 27–31 set out scope and definitions, including for the term 'law enforcement purposes', to which the data protection regime in this part would apply. This term is defined as follows:

> For the purposes of this part, "the law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.[60]

Clauses in this part also define 'competent authority' (providing a list in schedule 7), and specify that the intelligence services are not competent authorities within the meaning of this part.[61]

Clauses 32–40 set out the six data protection principles governing the processing of personal data for law enforcement purposes specified in the Bill. These principles require:

- Processing be lawful and fair.
- The purposes of processing be specified, explicit and legitimate.
- Personal data be adequate, relevant and not excessive.
- Personal data be accurate and kept up to date.
- Personal data be kept for no longer than is necessary.
- Personal data be processed in a secure manner.[62]

In addition, clauses 41–52 relate to the rights of the data subject, including right of access, rights to rectification or erasure and the right not to be subject to automated decision-making; clauses 53–69 relate to data controllers and processors; clauses 70–76 relate to transfers of personal data to third countries; and clauses 77–79 relate to supplementary matters including the restriction of certain rights of data subjects by certification of a Minister of the Crown for the purposes of national security and the reporting of infringements.[63]

Concern has been raised about the right of data subjects to request access to their personal data free of charge, in particular in relation to the resourcing implications for organisations that currently receive a low

---

[60] Clause 29.

[61] Clause 28 and schedule 7.

[62] Clauses 32–8; and Explanatory Notes, pp 31–3.

[63] Explanatory Notes, pp 40–1.

number of subject access requests (perhaps due to the cost barrier in place, currently a maximum of £10).[64]

2.4 Part 4: Intelligence Services Processing

Part 4 comprises clauses 80–111, which relate to the processing of personal data by the intelligence services (the Security Service, the Secret Intelligence Service and the Government Communications Headquarters).

Clauses 80–82 relate to scope and definitions. Clauses 83–89 relate to the data protection principles governing the processing of personal data by the intelligence services, which are identical to those principles applying to data processing for law enforcement purposes, with the addition that processing should be transparent in addition to being fair.[65] Clauses 90–98 relate to the rights of the data subject, including the right to information, right of access, right not to be subject to automated decision-making, right to information about decision-making, right to object to processing and rights to rectification and erasure; clauses 99–106 relate to the controllers and processors of data; clause 107 relates to transfers of personal data outside the United Kingdom; and clauses 108–111 relate to exemptions as required for the purpose of safeguarding national security.[66]

2.5 Part 5: The Information Commissioner

Part 5 consists of clauses 112–136 and covers provisions relating to the Information Commissioner. In particular, clauses in this part make provision for matters including:

- The continued existence of the Commissioner.
- That the Commissioner remain the supervisory authority for data protection in the UK under the GDPR in addition to other domestic functions.
- The Commissioner's international role in the context of an obligation on the Commissioner to engage with third countries and international organisations.
- Codes of practice, including a direct marketing code of practice.
- Consensual audits as a means of assessing whether a data controller or processor is complying with good practice.
- Information provided to the Commissioner.
- Fees that the Commissioner may charge.

---

[64] For example, see Martin Hoskins, 'The Future for "Free" Subject Access Requests', Data Protector Blog, 28 September 2017. The usual maximum fee that can be charged for a subject access request is £10 (Information Commissioner's Office, 'Subject Access Request', accessed 4 October 2017).

[65] Clause 84; and Explanatory Notes, p 43.

[66] Explanatory Notes, pp 47–8.

- Charges payable to the Commissioner by data controllers.
- Reports, including those compiled by the Commissioner to be laid before both Houses of Parliament.[67]

2.6 Part 6: Enforcement

Part 6 of the Bill is comprised of clauses 137–168 relating to relevant enforcement mechanisms. Provisions include those relating to the following:

- Information, assessment and enforcement notices.
- Powers of entry and inspection.
- Penalties, including the introduction of a new maximum penalty of €20 million or 4 percent of total worldwide turnover in the preceding financial year (whichever is higher—up from the current maximum fine of £500,000).
- Guidance about regulatory action.
- Appeals relating to notices, penalties and rulings from the Commissioner.
- Complaints to the Commissioner by data subjects about an infringement of the data protection legislation in relating to his or her personal data.
- Remedies in the court, including compensation.
- Offences relating to personal data, including the unlawful obtaining of personal data, re-identification or de-identified personal data and alteration of personal data to prevent discloser.
- Jurisdiction of courts in England and Wales, Northern Ireland and Scotland.[68]

As indicated above, this part would bring in new offences relating to personal data. These include the deliberate or reckless obtaining, disclosing and retention of personal data without the consent of the data controller; knowingly or recklessly re-identifying information that has been de-identified without the consent of the controller who de-identified the data; and the alteration of personal data to prevent disclosure following the exercise of a subject access right.[69]

---

[67] Explanatory Notes, pp 48–53.
[68] ibid, pp 54–64.
[69] Clauses 161–3; and Explanatory Notes, pp 62–3.

2.7 Part 7: Supplementary and Final Provision

Part 7 comprises clauses 169–194 and relates to supplementary and final provision. This includes:

- Regulations to be made under the Act.
- Changes to the CoE Data Protection Convention (Convention 108).
- Offences, including penalties and prosecution.
- Tribunals, including procedure rules.
- General matters including the application of provisions to the Crown and Parliament.[70]

3. Reaction to the Bill

3.1 Political Reaction

In August 2017, the Shadow Secretary of State for Digital, Culture, Media and Sport, Tom Watson, welcomed the Government's move to update the UK's data protection regime. However, he criticised the Government for a perceived delay in updating the law in this area. He stated:

> The Government opposed Labour's attempts to strengthen data protection laws during the passage of the Digital Economy Act just months ago, so it is welcome news that they've finally understood that our current data protection legislation needs updating.
>
> Labour's manifesto committed to allowing young people to remove content shared on the internet before they turned 18, so we're glad the Government is taking action on this.
>
> As we are leaving the EU it is more important than ever that we have a robust data protection framework fit for the future. We'll be scrutinising the bill carefully to make sure it creates that future proof framework.[71]

Similarly, Ed Davey, the Liberal Democrats' spokesperson on Home Affairs, welcomed the Bill, which he stated included a "raft of measures that will improve all our privacy online". However, he also criticised the Government

---

[70] Clauses 169–194; and Explanatory Notes, pp 65–71.

[71] Labour Party, 'Labour Welcome that the Government have Finally Understood that Our Current Data Protection Legislation Needs Updating', 7 August 2017.

for a perceived delay in taking action on the issue and for "trying to take credit for rules that were already agreed at EU level", adding:

> The reality is that adopting EU standards after Brexit will be crucial to allow UK digital firms to carry on handling data and trading easily across Europe.
>
> The Brexiteer myth that leaving the EU would mean regaining sovereignty is being exposed yet again.[72]

Data Protection is a reserved matter, and data protection was not mentioned in either the Scottish National Party (SNP) or Democratic Unionist Party (DUP) manifestos published ahead of the most recent general election.

3.2 Stakeholder Reaction

Information Commissioner

In a statement published on 14 September 2017, the same day as the Bill was published, Elizabeth Denham, the Information Commissioner since July 2016, welcomed the Bill, stating it would "put in place one of the final pieces of much needed data protection reform". She added:

> Effective, modern data protection laws with robust safeguards are central to securing the public's trust and confidence in the use of personal information within the digital economy, the delivery of public services and the fight against crime. I will be providing my own input as necessary during the legislative process.[73]

The day before, Ms Denham had set out her views on the UK-EU data protection relationship post-Brexit during a speech at the CBI Cyber Security Conference:

> I think we need to be as close to Europe as possible with our laws. I have been advocating for a legal arrangement post Brexit that provides for uninterrupted data flows.

---

[72] Liberal Democrats, 'The Government is Trying to Claim Credit for EU Rules', 7 August 2017.

[73] Information Commissioner's Office, 'Statement on the Data Protection Bill', 14 September 2017. In a speech delivered to the National Association of Data Protection and Freedom of Information Officers in November 2016, Ms Denham welcomed the update of data protection law represented by the GDPR and characterised its aim of giving consumers control over their data as a "positive development" ('127 Days in the Job and Preparing for GDPR', 21 November 2016).

> The Government's data protection partnership position paper, announced last month, is a positive step but the legal arrangement to provide for essential equivalency is critical for companies, law enforcement and for individual data subjects.[74]

Other Reaction

Speaking on the same day, Tom Thackray, Innovation Director at the Confederation of British Industry (CBI) also welcomed the Bill as a "crucial milestone in modernising the UK's data protection framework". He added:

> With the regulation due to be enforced from 25 May 2018, businesses in all sectors will want smooth progress through Parliament to ensure enough time for to prepare for the new legislation.[75]

Around the same time, it was reported that Josh Hardie, CBI Deputy Director General, had urged the Government to agree a transitional data protection deal with the EU, and to seek to secure an 'adequacy decision' in the long term, to protect the UK's estimated £240 billion data economy.[76]

The Open Rights Group, which describes itself as the "UK's only digital campaigning organisation working to protect the rights to privacy and free speech online", welcomed the Bill, though it criticised the Government for "fail[ing] to enact all of the options outlined in the GDPR".[77] Elaborating on this point, Jim Killock, Executive Director, stated:

> The UK has neglected an important option in the General Data Protection Regulation, which gives consumer privacy groups like Open Rights Group the ability to lodge independent data protection complaints.
>
> It is almost impossible for the average person to know how their data is being collected, shared and sold by social media platforms, advertisers and other businesses. We may not know which companies hold data about us. Privacy groups can therefore play an important role in protecting consumers by taking independent action against companies that fail to protect our data protection rights.

---

[74] Confederation of British Industry, 'Full Speech: Elizabeth Denham on Cyber Security and Data Protection', 13 September 2017.
[75] Confederation of British Industry, 'Data Protection Bill is a Crucial Milestone', 14 September 2017.
[76] Catherine Neilan, 'CBI Warns of Cliff Edge for £240bn Data Economy', *City AM*, 13 September 2017.
[77] Open Rights Group, 'About', accessed 4 October 2017; and 'Data Protection Bill Must Give Privacy Groups Right to Lodge Complaints', 14 September 2017.

> Open Rights Group wants to be able to campaign on behalf of people who are afraid of complaining or do not realise that they have been affected.[78]

It has also been reported that journalists, academics, researchers and employers have raised concerns that some of the rights introduced or reinforced by the Bill could be used to "suppress freedom of expression, the ability to carry out research, or the right to run background checks on prospective employees".[79] However, the Government has indicated that such groups, as well as the bodies tasked with catching drug cheats in sport, would be shielded by provisions in the Bill.

4. Further Information

This briefing should be read in conjunction with the detailed Explanatory Notes to the Bill, produced by the Department for Digital, Culture, Media and Sport. In addition, the following documentation may be of assistance for further background information:

- Department for Digital, Culture, Media and Sport, Collection: Data Protection Bill 2017, 14 September 2017 (includes, *Data Protection Bill Factsheet: Overview*; *Data Protection Bill: Impact Assessment*; *Data Protection Bill Factsheet: General Data Processing (Clauses 3–26)*; *Data Protection Bill Factsheet: Law Enforcement Data Processing (Clauses 27–79)*; *Data Protection Bill Factsheet: National Security Data Processing (Clauses 80–111)*; *Council of Europe: Draft Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*; and *Data Protection Bill Factsheet: The Information Commissioner and Enforcement (Clauses 112–168)*)
- Information Commissioner's Office, 'Data Protection Reform', accessed 26 September 2017
- JP Buckley, 'The Data Protection Bill: Are You Ready?', Shoosmiths LLP, 15 September 2017
- Robin Hopkins, 'The Data Protection Bill: Some Initial Observations', Panopticon Blog, 18 September 2017
- Robin Hopkins, 'The Data Protection Bill: A Brief Overview', Thomson Reuters Practical Law, 25 September 2017
- House of Commons Library, *Brexit and Data Protection*, 27 July 2017

---

[78] Open Rights Group, 'Data Protection Bill Must Give Privacy Groups Right to Lodge Complaints', 14 September 2017.
[79] Barney Thompson, 'UK Data Protection Rules to Exempt Journalists and Researchers', *Financial Times (£)*, 14 September 2017.

- House of Lords European Union Committee, *EU Data Protection Law: A 'Right to be Forgotten'?*, 30 July 2014, HL Paper 40 of session 2014–15; *Government Response*, 3 October 2014; and *European Commission Response*, 31 October 2014
- House of Commons Justice Committee, *The Committee's Opinion on the European Union Data Protection Framework Proposals*, 1 November 2012, HC 572 of session 2012–13
- Ministry of Justice, *Government Response to Justice Select Committee's Opinion on the European Union Data Protection Framework Proposals*, 11 January 2013, Cm 8530