

DATA PROTECTION BILL [HL]

EXPLANATORY NOTES

What these notes do

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66).

- These Explanatory Notes have been prepared by the Department for Digital, Culture, Media and Sport in order to assist the reader of the Bill and to help inform debate on it. They do not form part of the Bill and have not been endorsed by Parliament.
- These Explanatory Notes explain what each part of the Bill will mean in practice; provide background information on the development of policy; and provide additional information on how the Bill will affect existing legislation in this area.
- These Explanatory Notes might best be read alongside the Bill. They are not, and are not intended to be, a comprehensive description of the Bill.

Table of Contents

Subject	Page of these Notes
Overview of the Bill	7
Policy background	7
General Data Protection Regulation	8
Definitions and scope	8
Data protection principles	8
Lawfulness of processing	9
Individuals' rights	10
General processing	12
Definitions	12
Lawfulness of processing	12
Individuals' rights	13
Other general processing	14
Law enforcement processing	14
Intelligence services processing	16
The Information Commissioner, enforcement and offences	16
Legal background	17
General processing	17
Law enforcement processing	18
Intelligence services processing	19
Parliamentary scrutiny	19
Territorial extent and application	20
Commentary on provisions of Bill	21
Part 1: Preliminary	21
Clause 1: Overview	21
Clause 2: Terms relating to processing of personal data	21
Part 2: General processing	21
Chapter 1: Scope and definitions	21
Clause 3: Processing to which this Part applies	21
Clause 4: Definitions	21
Chapter 2: The GDPR	22
Clause 5: Meaning of "controller"	22
Clause 6: Meaning of "public authority" and "public body"	22
Clause 7: Lawfulness of processing: public interest etc	22
Clause 8: Child's consent in relation to information society services	22
Clause 9: Special categories of personal data and criminal convictions etc data	23
Clause 10: Special categories of personal data etc: supplementary	24
Clause 11: Limits on fees that may be charged by controllers	24
Clause 12: Obligations of credit reference agencies	25
Clause 13: Automated decision-making authorised by law: safeguards	25

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

Clause 14: Exemptions etc	26
Clause 15: Power to make further exemptions etc by regulations	26
Clause 16: Accreditation of certification providers	26
Clause 17: Transfers of personal data to third countries	27
Clause 18: Processing for archiving, research and statistical purposes: safeguards	28
Chapter 3: Other general processing	28
Clause 19: Processing to which this Chapter applies	28
Clause 20: Application of the GDPR to processing to which this Chapter applies	28
Clause 21: Power to make provision in consequence of regulations related to the GDPR	29
Clause 22: Manual unstructured data held by FOI public authorities	29
Clause 23: Manual unstructured data used in longstanding historical research	29
Clauses 24 to 26: National security	29
Part 3: Law Enforcement processing	30
Chapter 1: Scope and definitions	30
Clause 27: Processing to which this Part applies	30
Clauses 28 to 31: Definitions	30
Chapter 2: Principles	31
Clauses 32 to 40 and Schedule 8: Data protection principles	31
Chapter 3: Rights of the Data Subject	34
Clause 41: Overview and scope	34
Clause 42: Information: controller's general duties	34
Clause 43: Right of access by the data subject	34
Clauses 44 to 46: Data subject's rights to rectification or erasure etc	35
Clauses 47 and 48: Automated individual decision-making	35
Clauses 49 to 52: Supplementary	35
Chapter 4: Controller and processor	36
Clause 53: Overview and scope	36
Clauses 54 to 63: General obligations	36
Clause 64 and 65: Obligations relating to security	38
Clause 66: Communication of a personal data breach to the data subject	38
Clauses 67 to 69: Data protection officers	38
Chapter 5: Transfers of personal data to third countries etc	38
Clause 70: Overview and interpretation	38
Clauses 71 to 74: General principles for transfers	39
Clause 75: Transfers of personal data to persons other than relevant authorities	40
Clause 76: Subsequent transfers	40
Chapter 6: Supplementary	40
Clause 77: National security: certificates by the Minister	40
Clause 78: Special processing restrictions	41
Clause 79: Reporting of infringements	41
Part 4: Intelligence services processing	41
Chapter 1: Scope and definitions	41
Clauses 80 to 82: Processing to which this Part applies and definitions	41
Chapter 2: Principles	43
Clauses 83 to 89 and Schedules 9 and 10: Data protection principles	43
Chapter 3: Rights of data subjects	44
Clause 90: Overview	44
Clause 91: Right to information	44
Clauses 92 and 93: Right of access	44
Clauses 94 to 96: Rights related to decision-making	45
Clause 97: Right to object to processing	45
Clause 98: Right to rectification or erasure	45

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

Chapter 4: Controller and processor	46
Clause 99: Overview	46
Clauses 100 to 104: General obligations of controllers and processors	46
Clause 105: Security of processing	46
Clause 106: Communication of personal data breach	47
Chapter 5: Transfers of personal data outside the United Kingdom	47
Clause 107: Transfers of personal data outside the United Kingdom	47
Chapter 6: Exemptions	47
Clause 108 and 109: National security	47
Clauses 110 and 111 and Schedule 11: Other exemptions	48
Part 5: The Information Commissioner	48
Clause 112: The Information Commissioner	48
Clause 113: General functions under the GDPR and safeguards	48
Clause 114: Other general functions	48
Clause 115: Competence in relation to courts etc	49
Clause 116: Co-operation and mutual assistance	49
Clause 117: Inspection of personal data in accordance with international obligations	49
Clause 118: Further international role	49
Clause 119: Data-sharing code	49
Clause 120: Direct marketing code	50
Clause 121: Approval of data-sharing and direct marketing codes	50
Clause 122: Publication and review of data-sharing and direct marketing codes	50
Clause 123: Effect of data-sharing and direct marketing codes	50
Clause 124: Other codes of practice	50
Clause 125: Consensual audits	51
Clause 126: Disclosure of information to the Commissioner	51
Clause 127: Confidentiality of information	51
Clause 128: Guidance about privileged communications	51
Clause 129: Fees for services	52
Clause 130: Manifestly unfounded or excessive requests by data subjects etc	52
Clause 131: Guidance about fees	52
Clause 132: Charges payable to the Commissioner by controllers	52
Clause 133: Regulations under section 132: supplementary	52
Clause 134: Reporting to Parliament	53
Clause 135: Publication by the Commissioner	53
Clause 136: Notices from the Commissioner	53
Part 6: Enforcement	53
Clause 137: Information notices	53
Clause 138: Information notices: restrictions	53
Clause 139: Failure to comply with an information notice	54
Clause 140: Assessment notices	54
Clause 141: Assessment notices: restrictions	55
Clause 142: Enforcement notices	55
Clause 143: Enforcement notices: supplementary	56
Clause 144: Enforcement notices: rectification and erasure of personal data etc	56
Clause 145: Enforcement notices: restrictions	57
Clause 146: Enforcement notices: cancellation and variation	57
Clause 147: Powers of entry and inspection	57
Clause 148: Penalty notices	57
Clause 149: Penalty notices: restrictions	58
Clause 150: Maximum amount of penalty	58
Clause 151: Fixed penalties for non-compliance with charges regulations	59
Clause 152: Amount of penalties: supplementary	59
Clause 153: Guidance about regulatory action	59

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

Clause 154: Rights of appeal	59
Clause 155: Determination of appeals	59
Clause 156: Complaints by data subjects	60
Clause 157: Orders to progress complaints	60
Clause 158: Compliance orders	61
Clause 159: Compensation for contravention of the GDPR	61
Clause 160: Compensation for contravention of other data protection legislation	62
Clause 161: Unlawful obtaining etc of personal data	62
Clause 162: Re-identification of de-identified personal data	62
Clause 163: Alteration etc of personal data to prevent disclosure	63
Clause 164: The special purposes	63
Clause 165: Provision of assistance in special purposes proceedings	64
Clause 166: Staying special purposes proceedings	64
Clause 167: Jurisdiction	64
Clause 168: Interpretation of Part 6	64
Part 7: Supplementary and final provision	65
Clause 169: Regulations and consultation	65
Clause 170: Power to reflect changes to the Data Protection Convention	65
Clause 171: Prohibition of requirement to produce relevant records	65
Clause 172: Avoidance of certain contractual terms relating to health records	66
Clause 173: Representation of data subjects	66
Clause 174: Data subject's rights and other prohibitions and restrictions	66
Clause 175: Penalties for offences	66
Clause 176: Prosecution	67
Clause 177: Liability of directors etc	67
Clause 178: Recordable offences	67
Clause 179: Guidance about PACE codes of practice	67
Clause 180: Disclosure of information to the Tribunal	68
Clause 181: Proceedings in the First-tier Tribunal: contempt	68
Clause 182: Tribunal Procedure Rules	68
Clause 183: Meaning of "health professional" and "social work professional"	68
Clause 184: Other definitions	69
Clause 185: Index of defined expressions	69
Clause 186: Territorial application of this Act	69
Clause 187: Children in Scotland	69
Clause 188: Application to Crown	70
Clause 189: Application to Parliament	70
Clause 190: Minor and consequential amendments	70
Clause 191: Commencement	70
Clause 192: Transitional provision	70
Clause 193: Extent	70
Clause 194: Short title	71
Schedule 1: Special categories of personal data and criminal convictions etc data	71
Part 1 - Conditions relating to employment, health, research etc	71
Part 2 - Substantial public interest conditions.	72
Part 3 - Conditions for processing relating to criminal convictions etc	74
Part 4 - Additional Safeguards	74
Schedule 2: Exemptions etc from the GDPR	75
Part 1 - Adaptations and restrictions based on Articles 6(3) and 23(1) of the GDPR	75
Part 2 - Restrictions based on Article 23(1): General	75
Part 3 - Restrictions based on Article 23(1) in other circumstances	76
Part 4 - Restrictions based on Article 23(1): Restrictions of Rules in Articles 13 to 15	76
Part 5 - Exemptions etc based on Article 85(2) for reasons of freedom of expression and information	77
Part 6 - Derogations etc based on Article 89 for research, statistics and archiving	77

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

Schedule 3: Exemptions etc from the GDPR: health, social work, education and child abuse	78
Schedule 4: Exemptions etc from the GDPR: Disclosure prohibited or restricted by an enactment	79
Schedule 5: Accreditation of certification providers: reviews and appeals	79
Schedule 6: The applied GDPR and applied Chapter 2	79
Schedule 7: Competent authorities	84
Schedule 8: Conditions for sensitive processing	84
Schedule 9: Conditions relevant for purposes of the first principle: any processing	84
Schedule 10: Conditions relevant for purposes of the first principle: sensitive processing	84
Schedule 11: Other exemptions	84
Schedule 12: The Information Commissioner	85
Schedule 13: Other general functions of the Commissioner	86
Schedule 14: Cooperation and mutual assistance	86
Schedule 15: Powers of entry and inspection	87
Schedule 16: Penalties	88
Schedule 17: Relevant records	89
Schedule 18: Minor and consequential amendments	89
Commencement	91
Financial implications of the Bill	91
Parliamentary approval for financial costs or for charges imposed	91
Compatibility with the European Convention on Human Rights	91
Article 6: Right to a fair trial	91
Article 8: Right to respect for private and family life	92
Article 10: Freedom of expression	93
Related documents	94
Annex A – Glossary	95
Annex B – LED Transposition Table	96
Annex C – Convention 108	104
Annex D – Territorial extent and application in the United Kingdom	106
Minor or consequential effects	108
Subject matter and legislative competence of devolved legislatures	108

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

Overview of the Bill

- 1 The Bill implements a commitment in the 2017 Conservative Party manifesto to repeal and replace the UK's existing data protection laws to keep them up to date for the digital age in which ever increasing amounts of personal data are being processed. It sets new standards for protecting personal data, in accordance with recent EU data protection laws, giving people more control over use of their data. The Bill also helps prepare the UK for a future outside the EU.
- 2 The four main matters provided for in the Bill are general data processing, law enforcement data processing, data processing for national security purposes including processing by the intelligence services and regulatory oversight and enforcement.

Policy background

- 3 Data protection is needed to protect "personal data" which comprises data which relates to a living individual who can be identified from that data. The current law on data protection is found in the [Data Protection Act 1998](#) ("the 1998 Act"), which regulates the processing of personal data. The 1998 Act protects the rights of individuals whom the data is about. The Bill updates these rights to make them easier to exercise and to ensure they continue to be relevant with the advent of more advanced data processing than today's technology is capable of.
- 4 The Data Protection Bill ("the Bill") will replace the 1998 Act to provide a comprehensive legal framework for data protection in the UK, supplemented by the GDPR until the UK leaves the EU.
- 5 The Bill was announced in the Queen's speech on 21 June 2017. It will implement commitments to update data protection laws made in the 2017 Conservative Manifesto. The Bill modernises data protection laws in the UK to meet the needs of our increasingly digital economy and society. On the 24 August 2017 the Government published '[The exchange and protection of personal data – a future partnership paper](#)' setting out why the free flow of data is essential to the UK in future trading relationships.
- 6 While the UK remains a member of the EU, all the rights and obligations of EU membership remain in force. When the UK leaves the EU, the GDPR will be incorporated into the UK's domestic law under the European Union (Withdrawal) Bill, currently before Parliament.
- 7 Personal data is increasingly stored, processed and exchanged on the internet and as such often exists in an international environment. It is therefore necessary for data protection standards to be consistent at an international level. The Council of Europe [Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data](#) ("Convention 108") was signed by the UK on 14 May 1981. The Convention is open for all countries to sign, including states that are not members of the Council of Europe. On 1 November 2017, Tunisia will become the 51st Party to the Convention. The Council of Europe is in the process of preparing a [modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data](#) ("modernised Convention 108").
- 8 The UK's data protection laws, therefore, need to interlock with international data protection arrangements. The 1998 Act implemented the European Data Protection Directive (Directive 95/46/EC). On 25 May 2018 the Directive will be replaced when the [General Data Protection Regulation \(\(EU\) 2016/679\)](#) ("the GDPR") applies.

- 9 The Bill is structured in seven parts. Part one contains preliminary matters. Part two contains provision extending the GDPR standards to areas outside EU competence (the “applied GDPR” scheme), with the exception of law enforcement and processing by the intelligence services. The Bill and the GDPR apply substantively the same standards to the majority of data processing in the UK, in order to create a clear and coherent data protection regime. It also sets out certain derogations that provide exemptions from the GDPR. Part three contains provision for law enforcement data processing and Part four provides likewise for data processing by the intelligence services. The remaining parts provide for the continuance of the Information Commissioner (the “Commissioner”), enforcement and offences, and supplementary provision.

General Data Protection Regulation

- 10 To fully understand the Government’s legislative intent as found in this Bill, it may be necessary to have some wider background understanding of the GDPR.

Definitions and scope

- 11 The GDPR changes some of the definitions that set the scope of data protection law. Like the 1998 Act, the GDPR applies to “personal data”. The GDPR’s definition is more detailed and makes it clear that information such as an online identifier, for example a computer’s IP address, can be personal data. The more expansive definition expressly provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people. Also, personal data that has been pseudonymised, for example key-coded data, can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.
- 12 The 1998 Act provides additional safeguards for “sensitive personal data” which includes personal data relating to race, political opinion, trade union membership, health, sex life and criminal records. The GDPR refers to sensitive personal data as “special categories of personal data”. This extends the additional safeguards to specifically include genetic data, and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions etc. is not included, but processing of this data outside of the control of official authority must be authorised by domestic law, which provides for safeguards.

Data protection principles

- 13 The 1998 Act sets out eight data protection principles and these are largely carried over to the GDPR as set out in the table below. The GDPR also provides a new accountability principle.

	Data Protection Act principles	General Data Protection Regulation principles
<i>Lawfulness</i>	i. Personal data shall be processed fairly and lawfully and according to conditions.	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
<i>Purpose</i>	ii. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
<i>Data minimisation</i>	iii. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

<i>Accuracy</i>	iv. Personal data shall be accurate and, where necessary, kept up to date.	Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
<i>Storage</i>	v. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
<i>Access</i>	vi. Personal data shall be processed in accordance with the rights of data subjects.	The GDPR does not have an equivalent principle. Instead access rights are found separately in Chapter III of GDPR.
<i>Security</i>	vii. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
<i>Overseas transfer</i>	viii. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data	The GDPR does not have an equivalent principle. Instead overseas transfers of personal data are addressed separately in Chapter V.
<i>Accountability</i>	The 1998 Act does not have an equivalent principle.	The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Lawfulness of processing

- 14 The primary means of acquiring a lawful basis to process personal data under the GDPR is to obtain the consent of the individual to whom the data relates. Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action. Consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and it is also a requirement to provide simple ways for people to withdraw consent.
- 15 Persons giving consent need to have a certain level of understanding of what they are being asked which is why the GDPR specifies that parents or guardians must give consent to personal data processing on behalf of young children using information society services. "Information society services" generally include commercial websites. The term is defined as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services (see Article 1(1)(b) of EU Directive 2015/1535).

- 16 Consent is not the only way to enable processing of data. There may also be a contractual or other legal obligation that allows data to be processed without explicit consent. Data may be processed without consent where necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- 17 As with the 1998 Act, data may also be processed where there is a “legitimate interest”, although this can no longer be relied upon by public authorities. A legitimate interest may include processing for direct marketing purposes or preventing fraud; transmission of personal data within a group of undertakings for internal administrative purposes, including client and employee data processing for the purposes of ensuring network and information security and reporting possible criminal acts or threats to public security to a competent authority.
- 18 Where explicit consent is not obtained, there are even more restrictive limitations on when data can be lawfully processed for special categories of personal data and criminal data.

Individuals’ rights

- 19 The rights that individuals have over their data in the 1998 Act are carried over to the GDPR, but in some cases these are strengthened and have been added to as set out in the table below.

	Data Protection Act rights	General Data Protection Regulation rights
<i>The right to be informed</i>	<p>The Act provides the right to ‘fair processing information’, typically given through a privacy notice. The information must include:</p> <ul style="list-style-type: none"> the identity of the data controller, if the controller has nominated a representative, the identity of that representative, the purpose or purposes for which the data are intended to be processed, and any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair. 	<p>The GDPR sets out the information that should be supplied and when individuals should be informed. The GDPR specifies additional information than that under the 1998 Act that should be supplied at Articles 13 and 14.</p>
<i>The right of access</i>	<p>The Act provides that an individual who makes a written request and pays a fee is entitled to be: told within 40 days whether any personal data is being processed; given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people; given a copy of the information comprising the data; and given details of the source of the data.</p>	<p>The GDPR provides a similar right but the information must be provided for free although a ‘reasonable fee’ may be applied when a request is manifestly unfounded or excessive, particularly if it is repetitive. The time limit to respond is one month, or three months in complex cases.</p>
<i>The right to rectification</i>	<p>Where it is inaccurate, the individual concerned has a right to apply to the</p>	<p>Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. It must</p>

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

	court for an order to rectify, block, erase or destroy the inaccurate information.	be done within one month, or three months in complex cases. Where no action is taken individuals have the right to be informed of how to seek a judicial remedy.
<i>The right to erasure</i>	The Act does not provide the right to erasure, but an individual can apply to a court for an order for erasure of inaccurate personal data.	<p>Individuals have a right to have personal data erased in specific circumstances:</p> <ul style="list-style-type: none"> • where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed; • when the individual withdraws consent; • when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing; • when the personal data was unlawfully processed; • when the personal data has to be erased in order to comply with a legal obligation; or • when the personal data is processed in relation to the offer of information society services to a child.
<i>The right to restrict processing</i>	The Act allows individuals to apply to a court for an order to block or suppress processing of personal data where it is inaccurate. When processing is restricted, it is permissible to store the personal data, but not further process it.	Where it is claimed that data is inaccurate or the right to erasure has been exercised individuals can require the controller to restrict processing until verification checks have been completed. Individuals may also require controllers to restrict processing where there is no legal basis it is only needed for legal claims,
<i>The right to data portability</i>	Not applicable	<p>The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.</p> <p>It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.</p> <p>The personal data must be provided in a structured, commonly used and machine readable form. The information must be provided free of charge.</p>
<i>The right to object</i>	The Act provides individuals with the right to object to the processing of personal data for direct marketing.	In addition to direct marketing, individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling), and processing for purposes of scientific/historical research and statistics.
<i>Rights in relation to automated</i>	The Act allows an individual access to information about the reasoning behind	The GDPR provides similar rights and additionally defines profiling as any form of

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

<i>decision making and profiling</i>	any decisions taken by automated means. An individual can give written notice requiring that automated decisions are not made using their personal data. Individuals can ask for a decision taken by automated means to be reconsidered.	automated processing intended to evaluate certain personal aspects of an individual.
--------------------------------------	--	--

General processing

- 20 Chapter 2 of Part 2 of the Bill exercises a number of available derogations within the GDPR. On 12 April 2017 the Government published '[Call for views on the General Data Protection Regulation derogations](#)' and on 7 August 2017 the responses received were published, together with a Statement of Intent.

Definitions

- 21 The key terms used in the GDPR are largely consistent with the 1998 Act but the Bill makes use of derogations where it is possible to achieve further consistency. Article 4(7) of the GDPR defines what is meant by a 'controller' as the legal or natural person that determines the purposes and means of the processing of personal data. This is similar to the 1998 Act, but section 1(4) of the 1998 Act goes further by clarifying who is the controller when processing is required under an enactment. The Bill ensures that the clarity in section 1(4) is preserved.
- 22 The term 'public authority' is not defined in the GDPR. For clarity and legal certainty the Bill adopts the definitions in the Freedom of Information Act 2000 ("the 2000 Act") and the Freedom of Information (Scotland) Act 2002.

Lawfulness of processing

- 23 The Bill is drafted to ensure that existing data processing can continue, subject to the enhanced rights provided by the GDPR.
- 24 Persons giving consent to the processing of personal data need to have a certain level of understanding of what they are being asked which is why the GDPR specifies that parents or guardians must give consent to personal data processing on behalf of young children using information society services. The GDPR allows the UK to set the threshold for the minimum age at which a child can consent to such data processing to any age between 13 years and 16 years. The 1998 Act is silent on this matter but the Commissioner's guidance suggests, "Some form of parental consent would normally be required before collecting personal data from children under 12". As drafted, the Bill allows a child aged 13 years or older to consent to his or her personal data being processed by providers of information society services.
- 25 Processing of special categories of personal data (data concerning race, political opinions, health, etc. as described above) is generally prohibited unless explicit consent is obtained. However, the GDPR allows processing to take place in certain circumstances without consent and enables domestic law to stipulate the conditions and safeguards around this processing in certain cases. The processing of special categories of data and criminal conviction and offences data must be undertaken with adequate and appropriate safeguards to ensure the absolute protection of individuals' most sensitive personal data. There are many circumstances where this sort of data is legitimately used including the pricing of risk in financial services and the operation of anti-doping programmes in sport. The Bill replicates the current provisions in the 1998 Act that allow the processing of this sort of data. The Bill provides equivalent provision as far as possible to allow for continued processing for 'substantial public interest' purposes, to ensure that organisations are able to continue lawfully processing data whilst also achieving a balance between individuals' rights. The Bill aims to largely preserve the effect of paragraph 5 of Schedule 2 and of Schedule 3 to the 1998 Act as well as the Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 2000/417).

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

- 26 It is not possible to predict what future circumstances may arise which justify the processing of these particularly sensitive categories of data without explicit consent of the individual. For example, in 2009 the then Home Secretary established the Hillsborough Independent Panel to investigate the disaster which occurred on 15 April 1989. Some of the information held by public bodies within the scope of the Hillsborough disclosure exercise included sensitive personal data so the Secretary of State made the Data Protection (Processing of Sensitive Personal Data) Order 2012 (SI 2012/1978) to ensure that there was no room for doubt that it may be possible in an appropriate case for an individual or body to disclose such data. The Bill provides the Secretary of State with the necessary power to manage unforeseeable situations of this sort.
- 27 The GDPR gives individuals the right to object to decisions made about them solely on the basis of automated processing, where those decisions have legal or other significant effects. This includes processing where there is no human intervention, for example, when data is collected about an individual's personal finances, which is then processed to calculate creditworthiness. The GDPR allows additional safeguards to protect consumers from inaccurate processing to be provided for in domestic legislation. The Bill replicates the additional safeguards provided within section 12(2) of the 1998 Act should continue to apply and the Bill makes appropriate provision.

Individuals' rights

- 28 There are some limited circumstances where it is appropriate to create exemptions to the usual rights that individuals have over personal data that relates to themselves. In the context of health, social work and education, there is sometimes information that is recorded about a person that is only given on the condition that it is not disclosed to the person. If all information was disclosable the information would not be given and this could result in safeguarding concerns. The 1998 Act and various orders made under powers in the Act provide exemptions to individuals' rights. For example, the Data Protection (Subject Access Modification) (Health) Order 2000 (SI 2000/413) applies to personal data consisting of information as to the physical or mental health or condition of the individual. It covers Court proceedings, essentially preserving the confidentiality of certain reports provided to the Court in proceedings concerned with the care of children. The Bill ensures that exemptions of this sort continue to apply.
- 29 The 1998 Act also contains exemptions to disapply individual rights in relation to personal data held by regulatory bodies such as watchdogs performing functions concerned with protecting the public from incompetence, malpractice, dishonesty or seriously improper conduct, or concerning health and safety; charities; or fair competition in business. Without appropriate exemptions a corrupt official might be able to find out how his or her corruption is being exposed. Similarly the Government believes that exemptions should continue to exist to ensure that the judiciary have a 'safe space' in which to conduct their work, where they are free to make such records as they see fit whilst reaching their judgment, without fear that such records (such as annotations, recorded discussions) may be investigated or challenged by parties to proceedings. The Bill ensures that exemptions of this sort are available.
- 30 In some cases, there are also public policy reasons to limit individual rights where there are on-going investigations into their conduct. While investigations by law enforcement agencies are not covered by GDPR and the Bill will make separate provision (see below), there are instances where other investigations may benefit from exemptions from the requirement to apply individual rights. For example, section 29(1) of the 1998 Act enables Her Majesty's Revenue and Customs ("HMRC") to withhold certain personal data on a case by case basis from an individual customer who submits a subject access request if providing that particular personal data would be likely to prejudice specified crime and taxation purposes. It also

means that HMRC is not obliged to send a specific privacy notice to an individual customer when they obtain personal data from a third party if it would tip the customer off about an ongoing investigation into their tax affairs. The Bill makes equivalent provision.

- 31 The 1998 Act provides that personal data processed only for research, historical or statistical purposes is exempt from subject access requests. The Bill exercises all of the derogations in Article 89(2) and (3) of the GDPR to ensure that research organisations and archiving services do not have to respond to subject access requests when this would seriously impair or prevent them from fulfilling their purposes. Further, the Bill contains provision to exercise derogations so that research organisations do not have to comply with an individual's rights to rectify, restrict further processing and object to processing where this would seriously impede their ability to complete their work, and providing that appropriate organisational safeguards are in place to keep the data secure. In effect, these derogations maintain the status quo.
- 32 As it is difficult to predict what matters may in future be considered important objectives of general public interest deserving protection, it is also difficult to predict what rights and obligations may need to be restricted in order to safeguard those objectives. The Bill therefore provides the Secretary of State with the power to make further exemptions in future.

Other general processing

- 33 Article 2(2) of the GDPR states that the Regulation does not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law. To avoid data controllers being compelled to do an assessment of whether the activity they are engaged in falls inside or outside the scope of Union law, the Bill contains provision to extend the GDPR standards to data processing, other than processing caught by Part 3 (law enforcement) or Part 4 (intelligence services), to create a simple framework under which data controllers and processors can apply a single standard.
- 34 The Bill achieves this by applying the relevant Articles of the GDPR to general data outside the scope of Union law as set out in Schedule 6 (the applied GDPR scheme). In applying the Articles of the GDPR, the Bill simultaneously makes some modifications to the Articles to make them relevant to a context where Union law does not apply. While it is appropriate to apply the limitations and safeguards on data processing as well as the associated rights, references to Member States and EU institutions cannot be relevant and are removed.
- 35 When the UK leaves the EU there will no longer be a distinction between general data inside and outside the scope of Union law. The Government's intention is that GDPR standards will continue to apply to data processing within the scope of Part 2. When the GDPR is brought within the UK's domestic law, using the powers in the European Union (Withdrawal) Bill the Government expects to make provision to enable a single domestic legal basis to apply the GDPR data processing standards.
- 36 The GDPR does not apply to national security data processing and the Bill provides national security exemptions for data processing outside the scope of Union law.

Law enforcement processing

- 37 National security is outside the scope of EU law. As a result, the processing of personal data in connection with national security activities and processing by agencies or units dealing with national security issues is not within scope of the GDPR or the Law Enforcement Directive. Domestic processing of personal data for law enforcement purposes is currently governed by the 1998 Act. The transmitting of personal data for law enforcement purposes between Member States of the European Economic Area ("EEA") is governed by the provisions of Part 4 of the Criminal Justice and Data Protection (Protocol No. 36) Regulations

2014 (SI 2014/3141) (“the 2014 Regulations”) which transposed into UK law [Council Framework Decision 2008/977/JHA](#)¹ of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. Part 4 of the 2014 Regulations established a legal framework which applies to competent authorities in EEA States when transmitting or making available personal data to competent authorities in other EEA States for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. In such cases, Part 4 of the 2014 Regulations applies instead of the 1998 Act, except as provided for by that Part.

- 38 The GDPR does not apply to the processing of personal data by competent authorities (broadly the police and other criminal justice agencies) “for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security” (see Article 2(2)(d)). Instead, alongside of the GDPR, the European Parliament and Council adopted the Law Enforcement [Directive \(EU\) 2016/680](#)² “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”.
- 39 Unlike the GDPR, this Law Enforcement Directive (“LED”) is not directly applicable EU law; accordingly Part 3 of the Bill (together with provisions in Parts 5 to 7 which apply across the GDPR, LED and intelligence services regimes) transposes the provisions of the LED into UK law.
- 40 The scope of the LED is provided for in Article 1 and concerns the processing of personal data by competent authorities for law enforcement purposes. A competent authority is any public authority competent for 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. Further, a competent authority may also be any other body or entity entrusted by Member State law to exercise public authority and public powers for 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. This definition covers not only all police forces, prosecutors and other criminal justice agencies in the UK, but also other organisations with law enforcement functions, such as Her Majesty’s Revenue and Customs, the Health and Safety Executive and the Office of the Information Commissioner.
- 41 While the LED only applies in relation to the cross-border processing of personal data for law enforcement purposes (see paragraph 57 below), Part 3 of the Bill also applies to the domestic processing of personal data for such purposes. This 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. The provisions of the GDPR, together with the derogations in Chapter 2 of Part 2 of the Bill, will apply to the processing of personal data by

¹ Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

² Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

law enforcement agencies for purposes other than law enforcement purposes, for example for internal personnel management/ human resources purposes.

- 42 Member States are required to adopt laws giving effect to the LED by 6 May 2018.

Intelligence services processing

- 43 Domestic processing of personal data by the intelligence services, comprising the Security Service, the Secret Intelligence Service and the Government Communications Headquarters, is currently governed by the 1998 Act. National security is outside the scope of EU law by virtue of Article 4(2) of the Treaty on European Union, which states that national security is the sole responsibility of each Member State. Therefore the processing of personal data in connection with national security activities and processing by agencies or units dealing with national security issues is not within scope of the GDPR, as a result of which the provisions of the GDPR were not designed to be applicable to the unique nature of intelligence service processing. Part 4 of the Bill therefore provides a data protection regime for the processing of personal data by the intelligence services based on the Council of Europe modernised, but yet to be agreed, Convention 108.
- 44 The 1998 Act is consistent with the current Convention 108 standards. Part 4 of the Bill will build on the existing regime by seeking to adopt the standards of the modernised Convention 108 to ensure processing of personal data carried out by the intelligence services will be in-line with anticipated future international standards. It provides for rules on processing personal data in the national security context whilst ensuring that the UK intelligence community can tackle existing, new and emerging national security threats.
- 45 As is the case currently under the 1998 Act, and consistent with that Act, the regime in Part 4 of the Bill will provide for adequate and proportionate exemptions from processing which can only be applied when necessary to safeguard national security. Also consistent with the 1998 Act there is provision for a certificate signed by a Minister of the Crown certifying that exemption from a specified requirement is necessary for the purpose of safeguarding national security to be conclusive evidence of that fact.
- 46 The intelligence services already comply with data handling obligations. These are supported by physical, technical and procedural controls which are overseen by the Investigatory Powers Commissioner and which are also aligned to the [Cabinet Office Transforming Government Security Review](#). They include vetting of personnel, handling restrictions based on classification of data, firewalling and air gapping of internal IT and access restrictions.
- 47 The regulatory structure applying to the intelligence services is found in other legislation and already imposes restrictions on their activities, including relating to their data handling practices. This includes the Security Services Act 1989, the Intelligence Services Act 1994, the Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016 (“the 2016 Act”). For example, Part 7 of the 2016 Act provides for agency specific warrants which are relevant to how the agencies hold and use bulk personal datasets. The 2016 Act also creates a number of offences which are applicable if an individual in an agency wrongly uses or discloses data obtained using the powers in that Act.

The Information Commissioner, enforcement and offences

- 48 The Commissioner heads the UK data protection supervisory authority. The Commissioner was originally the Data Protection Registrar as provided for by the Data Protection Act 1984. In the 1998 Act the office was renamed the Data Protection Commissioner and the 2000 Act established the current title for the post of Commissioner. The Bill repeals the 1998 Act and while the GDPR makes provision for the continuing existence of the supervisory authority,

there are some matters in the 1998 Act that need to be carried over and therefore the Bill contains relevant provision.

- 49 The powers of the Commissioner to investigate and sanction responsible persons have changed and grown over time as all types of data, including personal data, are capable of being accessed, analysed, transmitted, and stored in dramatically different ways to 30 years ago. Under the 1998 Act, as enacted, the Commissioner could only serve enforcement notices and her powers to impose fines only came in the Criminal Justice and Immigration Act 2008 which enabled the Commissioner to issue a civil monetary penalty notice of up to £500,000 in respect of the most serious breaches. The GDPR now extends this so that the Commissioner can in the most serious cases issue a maximum fine of £18 million (€20 million) or 4 per cent of turnover. The Bill ensures that the Commissioner's powers to issue fines are subject to certain safeguards, including as to the form of notice that is given, a right of appeal and information provided about how to exercise appeal rights.
- 50 Data protection law in the UK has always been accompanied by certain criminal offences relating to failure to comply with information notices, obtaining, disclosing or selling personal data without the data controller's consent and general offences relating to compliance with warrants and misconduct of the Commissioner's own officers. Most prosecutions are brought under section 55 of the 1998 Act, where a person knowingly or recklessly obtains, or discloses or procures, personal data without the data controller's consent. The maximum penalty is an unlimited fine. The Bill reproduces many of the criminal offences in the 1998 Act with modifications to account for changes to the legal framework brought by the GDPR and introduces some new offences to deal with emerging threats.
- 51 In June 2016, Dame Fiona Caldicott, the National Data Guardian for Health and Care published her [Review of Data Security Consent and Opt-Outs](#)³ recommending that the Government should criminalise the deliberate re-identification of individuals whose personal data is contained in anonymised data. On 1 March 2017, the Government published the [UK Digital Strategy](#)⁴ and committed to create a new offence along these lines. The Bill provides for such an offence.

Legal background

General processing

- 52 The Council of Europe "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" became open for signature in 1981. The Convention contained a set of principles to govern data processing, including that there should be fair and lawful obtaining and processing of personal data and storage of data only for specified purposes. In addition, states should not restrict trans-border data flows to other states which signed the Convention. States could only sign up to the Convention where they had national law in place guaranteeing compliance with the standards set out in it.
- 53 Accordingly, Parliament passed the Data Protection Act 1984 and ratified the Convention in 1985, partly to ensure the free movement of data. The Data Protection Act 1984 contained principles which were taken almost directly from Convention 108 - including that personal data shall be obtained and processed fairly and lawfully and held only for specified purposes.

³ National Data Guardian for Health and Care – Review of Data Security, Consent and Opt-Outs. 6 July 2016

⁴ UK Digital Strategy, Policy paper. 1 March 2017

- 54 The Data Protection Directive (95/46/EC) (“the 1995 Directive”) provides the current basis for the UK’s data protection regime. The 1995 Directive stemmed from the European Commission’s concern that a number of Member States had not introduced national law related to Convention 108 which led to concern that barriers may be erected to data flows. In addition, there was a considerable divergence in the data protection laws between Member States. The focus of the 1995 Directive was to protect the right to privacy with respect to the processing of personal data and to ensure the free flow of personal data between Member States.
- 55 The 1995 Directive was implemented in the UK through the 1998 Act which came into force on 1 March 2000. The 1998 Act repealed the Data Protection Act 1984. The scope of the 1998 Act is wider than the 1995 Directive, and covers all general data processing, including data processing for national security purposes, albeit with a broad exemption.
- 56 The 2000 Act introduced a new category of data which extended the definition of “data” in the 1998 Act to include any information held by a public authority which would not otherwise be caught by the definition. Public authorities must consider whether the release of information about identifiable individuals under a freedom of information request would breach the 1998 Act.
- 57 The GDPR was published in the [Official Journal of the European Union](#)⁵ on 4 May 2016 and directly applies on 25 May 2018. It replaces the 1995 Directive. Regulations do not normally require implementation as they are directly applicable as a result of Article 288 of the Treaty on the Functioning of the European Union (“TFEU”). In Case 39/72 Commission v Italy [1973] ECR 101 the court held it was wrong to duplicate the provisions of EU regulations in domestic law. The Bill therefore does not reproduce the text of the GDPR but instead exercises available derogations.

Law enforcement processing

- 58 The legal basis of the LED is Article 16(2) of the TFEU. Article 16 (which relates to the protection of personal data) measures in the area of police co-operation and judicial co-operation in criminal matters are subject to Article 6a of the UK (and Ireland’s) opt-in Protocol No. 21 for measures in Title V of the TFEU (which covers the Area of Freedom, Security and Justice). Article 6a provides that the UK (and Ireland) are not bound by rules laid down on the basis of Article 16 of the TFEU which relate to the processing of personal data by the Member States in certain circumstances. These are when carrying out activities which fall within the scope of Chapters 4 or 5 of Title V of the TFEU where the UK (and Ireland) are not bound by the rules governing the forms of judicial co-operation in criminal matters or police co-operation which require compliance with the provisions laid down on the basis of Article 16. The terms of Article 6a are reflected in recital 99 of the LED. Given this, the LED only applies to the UK in circumstances where data sharing is done under Title V measures in the area of police co-operation or judicial co-operation in criminal matters that bind the UK. For the reasons set out in paragraph 40 above, however, the provisions in Part 3 of the Bill apply to all processing – domestic and trans-national - for law enforcement purposes.

⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

- 59 In accordance with the Government's [Transposition Guidance](#)⁶, the approach taken in Part 3 of the Bill is broadly to copy-out the LED wherever possible and only to elaborate where such elaboration is necessary to reflect UK-drafting style, clarify the legal effect of a provision or to take advantage of flexibility afforded by the terms of the LED. Annex B to these Explanatory Notes contains transposition notes describing substantive departures from the text of the LED and the reasons for these.

Intelligence services processing

- 60 Convention 108 establishes a number of principles for states to transpose into their domestic legislation, these include the requirement to ensure that data is processed through procedures set out by law for a specific purpose, and data is stored no longer than is necessary for the intended purpose. An additional protocol requires each party to establish an independent authority to ensure compliance with data protection principles and lays down rules on trans-border data flows to non Parties.
- 61 In keeping with the Convention's philosophy, the provisions consist of general, simple and concise principles allowing signatories a certain measure of discretion when implementing them through national legislation.
- 62 The main innovations in the modernised Convention 108 will include:
- proportionality (formerly implicit);
 - accountability, in particular of data controllers and processors;
 - renewed focus on data security;
 - additional obligations to declare data breaches
 - enhanced transparency of data processing;
 - additional safeguards for the data subject such as the right not to be subject to a decision solely based on an automatic processing without having his or her views taken into consideration, the right to obtain information about the logic underlying the processing, and the right to object.
- 63 Article 9 of the modernised Convention 108 will continue to allow Parties to exempt controllers from some of these requirements for specified purposes. Of particular relevance for the intelligence services, one such purpose is the protection of national security.
- 64 The table at Annex C to these Explanatory Notes maps across the provisions of the draft modernised Convention 108 to the provisions of the Bill.

Parliamentary scrutiny

- 65 The GDPR and LED cleared scrutiny by the House of Commons European Scrutiny Committee (22nd Report of session 2015/16, [HC342-xxi](#)) and the House of Lords EU Select Committee (Progress of Scrutiny, 3rd edition session 2016/17, [EUC-3](#)) in February 2016. In addition the GDPR and LED were the subject of inquiries by the House of Commons Justice Committee (*The Committee's opinion on the European Union Data Protection framework proposals*, 3rd Report of session 2012/13, [HC 572](#)) and the House of Lords EU Home Affairs Sub-Committee (*Brexit: the EU data protection package*, [HL paper 7](#)).

⁶ Transposition Guidance: How to implement European Directives effectively

⁷ Brexit: the EU data protection package, 3rd Report of Session 2017-19, HL Paper 7

Territorial extent and application

- 66 Subject to minor exceptions, the Bill extends and applies to the whole of the UK. Clause 186 (recordable offences) extends and applies to England and Wales only.
- 67 There is a convention that Westminster will not normally legislate with regard to matters that are within the legislative competence of the Scottish Parliament, the National Assembly for Wales or the Northern Ireland Assembly without the consent of the legislature concerned. In relation to Scotland and Wales this convention is enshrined in law, see section 28(8) of the Scotland Act 1998 and section 107(6) of the Government of Wales Act 2006.
- 68 Under Part II B2 of Schedule 5 to the Scotland Act 1998, the subject matter of the Data Protection Act 1998 is a reserved matter. The scope of the Bill is consistent with the 1998 Act so in the Government's view, is also a reserved matter.
- 69 The subject matter of the 1998 Act is also a reserved matter under paragraph 40 of Schedule 3 to the Northern Ireland Act 1998.
- 70 Paragraph 2 of Part 2 of Schedule 7 to the Government of Wales Act 2006 explicitly prevents the National Assembly for Wales from introducing measures which modify the 1998 Act. Data protection does not fall within the subject matters devolved to Wales. Schedule 1 to the Wales Act 2017 provides for a new Schedule 7A to the Government of Wales Act 2006 which includes a specific reservation at paragraph 170 for personal data.
- 71 If there are amendments relating to matters within the legislative competence of the Scottish Parliament, the National Assembly for Wales or the Northern Ireland Assembly, the consent of the relevant devolved legislature(s) will be sought for the amendments.
- 72 See the table in Annex D for a summary of the position regarding territorial extent and application in the United Kingdom. The table also summarises the position regarding legislative consent motions and matters relevant to Standing Orders Nos. 83J to 83X of the Standing Orders of the House of Commons relating to Public Business.

Commentary on provisions of Bill

Part 1: Preliminary

Clause 1: Overview

73 This clause sets out the various Parts of the Bill and is self-explanatory.

Clause 2: Terms relating to processing of personal data

74 This clause defines key terms used in the Bill.

75 Part 2 of the Bill concerns general data and makes provision for those areas where the GDPR gives Member States a discretion on specific points and the Government wants to exercise that discretion, or where it is mandatory for Member States to make their own rules. To fully understand the Bill it is necessary to read it alongside the definitions found in the GDPR.

76 The Bill adopts and extends many of the definitions found in Article 4 of the GDPR. In particular the following definitions are adopted:

Term	GDPR Definition	Bill Definition
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.	Subsection (2) extends the GDPR definition to apply across the Bill.
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.	Subsection (4) extends the GDPR definition to apply across the Bill.
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.	Subsection (7) extends the GDPR definition to apply across the Bill.

Part 2: General processing

Chapter 1: Scope and definitions

Clause 3: Processing to which this Part applies

77 This clause specifies the types of data processing that applies under each Chapter within Part 2. Chapter 2 applies to data processing that falls within the scope of EU law. As the scope of GDPR is limited by the EU Treaty and consistent data processing standards for all general data processing is desirable, Chapter 3 applies to types of processing that is not within scope of EU law.

Clause 4: Definitions

78 This clause provides that terms used in Chapter 2 have the same meaning as in the GDPR, subject to any modifications in Chapter 2. It also provides that terms used in Chapter 3 have the same meaning as in the applied GDPR.

Chapter 2: The GDPR

Clause 5: Meaning of “controller”

- 79 This clause supplements the definition of “controller” found in Article 4(7) of the GDPR. This clause explains that when personal data is processed only for the purpose and means for which it is required by legislation to be processed, the person who has the obligation under that legislation to process the data is the data controller. This provision replicates section 1(4) of the 1998 Act.

Clause 6: Meaning of “public authority” and “public body”

- 80 Article 6(1)(a) to (f) of the GDPR sets out a list of conditions which allow for the lawful processing of personal data. Schedule 2 to the 1998 Act contained an equivalent provision to Article 6(1).
- 81 Article 6 (1)(e) makes reference to processing carried out by “public authorities in the performance of their tasks”. However, the GDPR does not provide a definition of “public authority” or “public body” for the purpose of Article 6 (1)(e) and Article 37.
- 82 This clause defines public authority and public body for the purpose of the GDPR and is consistent with the definition which existed in section 1(1) of the 1998 Act.
- 83 Subsection (1) provides a definition of “public authority” and “public body”, which applies to all references to these terms in the GDPR. The definition is based on that of a ‘public authority’ in the 2000 Act, and it applies to those bodies listed in Schedule 1 to the 2000 Act. A Scottish public authority is defined by the Freedom of Information (Scotland) Act 2002.
- 84 Subsection (2) contains a power for the Secretary of State to specify that a body is not a public authority, even if they are otherwise included in Schedule 1 to the 2000 Act.

Clause 7: Lawfulness of processing: public interest etc

- 85 Article 6(1)(e) of the GDPR provides that processing 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 vested in the controller. Article 6(2) of the GDPR enables Member States to, amongst other things, set out more specific provisions in respect of Article 6(1)(c) and (e).
- 86 This clause provides a non-exhaustive list of examples of processing under Article 6(1)(e). This includes processing of personal data that is necessary for the administration of justice, the exercise of a function of a Government department, either House of Parliament, the Crown, a Minister of the Crown or a function conferred on a person by enactment. The list is similar to that contained in paragraph 5 of Schedule 2 to the 1998 Act.

Clause 8: Child’s consent in relation to information society services

- 87 Article 8 of the GDPR sets the age at which a child can consent to the processing of their personal data by information society services. Information society services are defined as any service provided by electronic means, at a distance and at the individual request of a recipient of services and normally provided for remuneration, “remuneration” is likely to include receipt of revenues from advertising. “Information society services” cover more than just sites that involve buying and selling online. Most online websites would meet this definition, ranging from online banking to search engines and social media.
- 88 The GDPR gives Member States the flexibility to set this age provided that the age decided upon does not fall below age 13.
- 89 The Bill sets the age at which a child can give consent to the processing of data for the purposes of the provision of information society services at 13 years old. Any reference to age

16 in Article 8 of the GDPR, should be read as age 13 for the purposes of its application in the UK. This is in line with the minimum age set as a matter of contract by some of the most popular information society services which currently offer services to children (e.g. Facebook, Whatsapp, Instagram). This means children aged 13 and above would not need to seek consent from a guardian when accessing, for example, information society services which provide educational websites and research resources to complete their homework.

- 90 This clause clarifies the position in relation to preventative and counselling services and provides that references to information society services in Article 8 GDPR do not include preventative and counselling services.
- 91 The 1998 Act does not contain equivalent provision. As long as a child is capable of understanding the processing to which they are consenting and is capable of making a free and informed decision, then it is considered that the child is capable of consenting to any processing of personal data.
- 92 Likewise, the 1998 Act does not contain a reference to information society services, as this concept was first defined in the E-commerce Directive (2000/31/EC).

Clause 9: Special categories of personal data and criminal convictions etc data

- 93 Article 9(1) of the GDPR generally prohibits the processing of “special categories of data”. “Special categories of data” are defined in Article 9(1) of the GDPR as “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.
- 94 Article 9(2) of the GDPR provides for circumstances in which the prohibition on processing special categories of data in Article 9(1) may not apply. Some of these have direct effect and others take the form of derogations requiring Union or Member State law in order to be relied upon, subject to safeguards. Subsections (1) to (3) makes provision for processing of special categories of data in reliance on derogations contained in Article 9(2)(b), (g), (h), (i) and (j).
- 95 Article 10 of the GDPR allows for processing of personal data relating to criminal convictions or related security measures to be carried out under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of others. Subsections (4) and (5) permit the processing of this kind of personal data otherwise than under the control of official authority.
- 96 Subsection (1) introduces subsections (2) and (3), which make provision for the processing of special categories of personal data for reasons of employment, social security and protection (Article 9(2)(b)); substantial public interest (Article (2)(g)); health and social care (Article 9(2)(h)), public health (Article 9(2)(i)) and archiving, research and statistics (Article 9(2)(j)).
- 97 Subsection (2) provides that processing under Articles 9(2)(b), (h), (i) or (j) is only permitted by UK law if it meets a condition in Part 1 of Schedule 1.
- 98 Subsection (3) provides that processing under Article 9(2)(g) is only permitted by UK law if it meets a condition in Part 2 of Schedule 1.
- 99 Subsections (4) and (5) provide that processing of personal data relating to criminal convictions and offences or related security measures is only permitted by UK law if it meets a condition in Parts 1, 2 or 3 of Schedule 1.
- 100 Subsections (6) and (7) provide the Secretary of State with regulation-making powers to amend Schedule 1 by adding, varying or omitting processing conditions or safeguards as well

as powers to make consequential amendments to this section. These regulations are subject to the affirmative resolution procedure.

101 This clause does not reproduce all of the conditions found in Schedule 3 to the 1998 Act because many of these are now found in similar form in the GDPR and have direct effect, as demonstrated in the table below:

GDPR Article	Processing condition for special category of data	Equivalent provision in the 1998 Act
Article 9 (2)(a)	The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where prohibited by law.	Paragraph 1 of Schedule 3
Article 9 (2)(c)	Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent.	Paragraph 3 of Schedule 3
Article 9 (2)(d)	Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.	Paragraph 4 of Schedule 3
Article 9 (2)(e)	Processing relates to personal data which are manifestly made public by the data subject.	Paragraph 5 of Schedule 3
Article 9 (2)(f)	Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.	Paragraph 6 of Schedule 3

Clause 10: Special categories of personal data etc: supplementary

102 This clause makes supplementary provision relating to the processing of special categories of data and personal data relating to criminal convictions and offences or related security measures

103 Article 9(2)(h) provides a Member State derogation for the processing of special categories of data for specified health and social care purposes. Any processing under Article 9(2)(h) on the basis of Member State law must be subject to the conditions and safeguards in Article 9(3) GDPR (obligations of professional secrecy etc.). Clause 10(1) provides that for the purposes of Article 9(2)(h), the conditions and safeguards referred to in Article 9(3) include circumstances in which processing is carried out by, or under the supervision of, a health or a social work professional or by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law. “Health professional” and “social work professional” are defined for the purposes of this Bill in clause 183.

104 Subsection (2) contains a non-exhaustive definition of personal data relating to criminal convictions and offences or related security measures.

Clause 11: Limits on fees that may be charged by controllers

105 This clause provides details on how the Secretary of State may specify limits on the fees that a controller may charge for manifestly unfounded or excessive requests for information by a data subject, or for provision of further copies of information already provided. An example of an excessive request for information is one that repeats the substance of previous requests.

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

106 The Secretary of State may use regulations to require controllers to publish guidance about the fees they charge. The Secretary of State is able to specify what the guidance must include.

107 Regulations under this section are subject to the negative resolution procedure.

Clause 12: Obligations of credit reference agencies

108 This clause concerns the treatment of right of access requests by data subjects under Article 15 of the GDPR when the data controller is a credit reference agency.

109 Subsection (2) retains the effect of section 9(2) of the 1998 Act. It deems a data controller's obligations under Article 15 of the GDPR as limited to information concerning the data subject's financial standing unless the data subject has indicated a contrary intention.

110 Where the controller discloses personal data in pursuance of Article 15 of the GDPR, subsection (3) requires the disclosure to be accompanied by a statement informing the data subject of their rights under section 159 of the Consumer Credit Act 1974. This continues the position under section 9(3) of the 1998 Act.

Clause 13: Automated decision-making authorised by law: safeguards

111 This clause relates to Article 22 of the GDPR. It sets out additional safeguards that apply in relation to certain types of automated decision making, including profiling.

112 Article 22 of the GDPR provides data subjects with the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, unless it is:

- necessary for creation and performance of a contract between a data subject and data controller;
- authorised by law to which the data controller is subject and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or
- based on the data subject's explicit consent.

113 Automated decision-making is not defined in the GDPR, but a reference to it is included in the definition of "processing" in Article 4(2).

114 Profiling is a new term. It is defined in Article 4(4) as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

115 The GDPR does not set out what suitable safeguards are, though recital 71 suggests they should include:

- provision of specific information to the data subject; and
- right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after an assessment, and an opportunity to challenge the decision.

116 In the case of decisions referred to in paragraph 112(a) and (c) above, data controllers are required to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

- 117 This clause provides additional safeguards that apply in the case described at paragraph 111 (b), where the automated decision making is authorised by law to which the data controller is subject.
- 118 Subsection (4)(a) requires data controllers to inform the data subject when an automated decision has been made, as soon as reasonably practicable, in writing. Subsection 4(b) provides the data subject may request the controller to reconsider the decision, or take a new decision not based solely on automated processing. Subsection (4) is based on section 12(2) of the 1998 Act.
- 119 Subsection (5) requires data controllers to consider the request of the notice and notify data subjects of steps taken to comply with that notice, and the outcome of complying with the notice. Subsection (5) is based on section 12(3) of the 1998 Act.
- 120 Subsection (6) provides that the Secretary of State may, by regulations, provide for additional safeguards, where for example, developments in technology require it. This is based on section 12(5)(b) of the 1998 Act.

Clause 14: Exemptions etc

- 121 Subsections (1) to (4) of this clause are self-explanatory and signposts the relative restrictions to data subject rights under the GDPR.
- 122 Subsection (5) is a distinct signposting provision. National security is outside the scope of EU law, consequently the processing of personal data in connection with national security activities, and by agencies or units dealing with national security issues, is not within the scope of the GDPR. As a result, save where the provisions of Parts 3 (law enforcement processing) and 4 (Intelligence Services processing) apply, any processing of personal data in connection with safeguarding national security would fall to be governed by the applied GDPR scheme provided for in Chapter 3 of Part 2, subject to the appropriate application of the exemptions provided for in clause 24. Where national security is engaged, subsection (5) signposts data controllers, processors and others to the applied GDPR scheme.

Clause 15: Power to make further exemptions etc by regulations

- 123 This clause provides the Secretary of State with the power to make regulations altering the application of the GDPR under Articles 6(3), 23(1), 85(2) and 89, including amending or repealing any of the derogations contained in the Bill.
- 124 Regulations made under this clause are subject to the affirmative resolution procedure.

Clause 16: Accreditation of certification providers

- 125 Article 42 of the GDPR encourages Member States to establish data protection certification mechanisms for the purpose of demonstrating compliance with the requirements in the Regulation for data processing. Certificates can be issued by the supervisory authority or by certification bodies.
- 126 Under Article 43 of the GDPR, Member States must ensure any certification bodies are accredited by the relevant authorities. The Regulation empowers both the supervisory authority and the national accreditation body to accredit certification bodies, and sets out the criteria which must be taken into account.
- 127 This clause outlines the process and requirements for accrediting certification bodies to oversee the certification mechanisms outlined in Article 42.
- 128 A data controller or processor claiming to be certified under Article 42, but which has not been certified by a certification provider accredited by either of the two bodies specified in

this clause is likely to be in breach of the business and consumer protection provisions in the Business Protection from Misleading Marketing Regulations 2008 ([SI 2008/1276](#)) or the Consumer Protection from Unfair Trading Regulations 2008 ([SI 2008/1277](#)).

- 129 Subsection (2) provides the conditions that the Commissioner must meet to accredit a person as a certification provider.
- 130 Subsection (3) provides the conditions that the national accreditation body must meet to accredit a person as a certification provider; when the Commissioner has published a statement that the body may carry out such accreditation, which has not been withdrawn by notice.
- 131 Subsection (4) provides that such a statement can only be published where the Commissioner is satisfied that the national accreditation body meets any additional requirements established by the Commissioner under Article 43(1)(b) of the GDPR. The Commissioner is not required to specify additional requirements.
- 132 Subsection (5) provides for the validity of any accreditation carried out before publication of a notice under (2)(b) or (3)(b).
- 133 Subsection (6) introduces Schedule 5 which makes provision about reviews and appeals of decisions of the accreditation authorities.
- 134 Subsection (7) provides the national accreditation body with a power to charge fees in respect of its accreditation functions under the Bill.
- 135 Subsection (8) outlines that the national accreditation body must provide information to the Secretary of State relating to the accreditation it carries out under the GDPR.
- 136 Subsection (9) defines “certification provider” as meaning a person which issues certification for the purposes of Article 42 of the GDPR.
- 137 Subsection (9) also defines the national accreditation body as the same body as that in Article 4(1) of the Accreditation and Market Surveillance Regulation ((EC) No 765/2008).
- 138 There is no equivalent provision to Article 43 or 42 of the GDPR in the 1998 Act.

Clause 17: Transfers of personal data to third countries

- 139 Article 49(4) and (5) of the GDPR allows Member States to create domestic law in the absence of an adequacy decision with a third country (a state that is not a member of the EU or EEA) or international organisation. In the absence of an adequacy decision, domestic law can be created to:
- ensure personal data can be transferred internationally where necessary for important reasons of public interest, and
 - restrict the international transfer of personal data for important reasons of public interest.
- 140 This clause provides regulation-making powers for these circumstances. These are similar to the order-making powers currently provided under paragraph 4 of Schedule 4 to the 1998 Act.
- 141 Subsection (1) deals with the first circumstance. It allows the Secretary of State to specify through regulations when data transfers can take place to a third country or international organisation, in the absence of an adequacy decision or other appropriate safeguards, and when doing so is for important reasons of public interest.

142 Subsection (2) deals with the second circumstance. It allows the Secretary of State to specify through regulations limitations on data transfers to a third country or international organisation, in the absence of an adequacy decision and when such limitations are for important reasons of public interest. These regulations are subject to the negative resolution procedure.

Clause 18: Processing for archiving, research and statistical purposes: safeguards

143 Article 89(1) of the GDPR requires appropriate safeguards for the processing of data in support of archiving, scientific or historical research purposes and statistical purposes. The 1998 Act provided supplementary safeguards to also ensure that personal data must not be processed by researchers to support measures or decisions with respect to particular individuals, and must not be processed in such a way as will, or is likely to, cause substantial damage or distress to any data subject. This clause replicates these safeguards.

144 Subsection (1) confirms the scope of provision to processing which is necessary for archiving in the public interest, scientific or historical research purposes, and statistical purposes.

145 Subsection (2) sets out that processing personal data for scientific or historical research purposes, statistical purposes, or for archiving in the public interest is prohibited where the processing causes substantial damage or distress to the data subject, or where the data has been processed to support a decision being made about the subject. This clause is largely similar to section 33(1) of the 1998 Act.

Chapter 3: Other general processing

Clause 19: Processing to which this Chapter applies

146 The GDPR, does not apply to all processing of personal data within the UK because some types of processing are outside the scope of the GDPR. Article 2(2) of the GDPR deals with matters which are out of scope.

147 This Chapter provides for a separate regime to apply to processing in the UK which is outside the scope of the GDPR. Subsection (1) provides that this includes any processing which falls outside the scope of EU law, with the exception of processing which occurs for law enforcement and national security purposes. Those types of processing are covered by their own regimes in Parts 3 and 4 of this Bill.

148 Subsection (2) makes it clear that this regime also covers the processing of unstructured, manual data held by a FOI public authority. Such processing was regulated by the 1998 Act, but is not covered by the GDPR, so equivalent provision is needed.

149 Definitions of “automated and structured processing of personal data” and “manual unstructured processing of personal data” are set out in subsection (4). Subsection (5) defines the meaning of FOI public authority and subsections (6) and (7) define what is meant by the term ‘held by an FOI public authority’ for the purposes of this Chapter.

Clause 20: Application of the GDPR to processing to which this Chapter applies

150 To ensure that processing covered by the regime in this Chapter is subject to similar standards as processing under the GDPR, subsection (1) provides for Articles in the GDPR to be taken as if they were part of an Act forming part of UK domestic law. Subsection (2) provides that the interpretation of key GDPR terms set out in Chapter 2 should also apply for the purposes of this Chapter.

151 Subsections (3) to (5) make further provision about how the Articles in the GDPR should be interpreted for the purposes of this Chapter.

152 Subsection (4) introduces Schedule 6 which contains a series of modifications that are necessary for the GDPR Articles to apply to processing covered by this Chapter.

Clause 21: Power to make provision in consequence of regulations related to the GDPR

153 In the same way that certain provisions under the GDPR can be modified by the Secretary of State through Regulations, this clause provides an equivalent power for the modification of Regulations made under this regime. Subsections (3) to (5) provide further detail about the content and purpose of such Regulations and parliamentary procedure for approving revisions.

Clause 22: Manual unstructured data held by FOI public authorities

154 Although clause 19 extends the regime in Chapter 3 to manual unstructured data held by public authorities, the extension is only relevant to processing that is necessary for FOI public authorities to process such personal data in response to information requests by the subject. This replicates the position under the 1998 Act where such records could be disclosed to the subject, where appropriate, but were exempt from most of the rights and duties created by the 1998 Act. Subsection (1) provides that the GDPR provisions listed in subsection (2) do not apply to manual unstructured personal data held by FOI public authorities. This effectively dis-applies the overarching GDPR principles and specified rights of data subjects which are not relevant to the unstructured manual records, such as the right to data portability.

155 Subsections (3) and (4) disapply further subject access rights in relation to unstructured manual data where it relates to personnel matters in connection with service in the armed forces, for the Crown or for a Government department.

156 Subsection (5) provides that data controllers are not obliged to comply with a data subject access request if the request omits a description of the personal data, or if the controller estimates that complying with the request would exceed the maximum cost. Subsection (6) provides, however, that this does not remove the controller's obligation to confirm whether or not personal data concerning the data subject is being processed, unless that in itself would exceed the appropriate maximum cost.

157 Subsection (7) explains how estimates of cost will be arrived at.

158 Subsections (8) and (9) allow the Secretary of State to specify the appropriate maximum cost in regulations, which are subject to the negative resolution procedure.

Clause 23: Manual unstructured data used in longstanding historical research

159 This clause provides that the listed GDPR provisions do not apply to manual unstructured data used in longstanding historical research. The provisions contained within Chapter II (principles) and Chapter III (rights of the data subject) of the GDPR do not apply when personal data was processed before 24 October 1998 or processed for the purposes of historical research, providing it is not carried out for measures or decisions to an individual, or likely to cause substantial damage or distress to the subject. The limit of 24 October 1998 is consistent with the 1998 Act.

160 This clause also provides that exemptions in clause 22 on manual unstructured data held by Freedom of Information public authorities also apply.

Clauses 24 to 26: National security

161 These clauses create an exemption from certain provisions in the applied GDPR scheme and in Parts 5, 6 and 7 of the Bill if that exemption is required for the purpose of safeguarding national security or for defence purposes. The provisions from which there is an exemption

are those listed in subsection (2) of clause 24 and include most of the data protection principles, the rights of data subjects, certain obligations on data controllers and processors, and various enforcement provisions.

162 This exemption is similar to the provision in section 28 of the 1998 Act which provided for exemptions. As now, a Minister of the Crown (as defined in clause 25(10)) may certify that an exemption is required in respect of specified personal data or processing. Clause 25(1) provides that such a certificate is to be taken as conclusive evidence of the exemption being required. A certificate issued by a Minister of the Crown is a means to give a data controller legal certainty that an exemption applies to the specified data processing.

163 Any person directly affected by the issuing of any certificate may appeal to the tribunal to judicially review the decision to issue the certificate (clause 25(3) and (4)). A party to proceedings may also challenge the application of a certificate to the processing of particular personal data (clause 25(5)).

164 Clause 26 modifies the application of Articles 9 (prohibition on processing of special categories of personal data) and 32 (security of processing) of the applied GDPR scheme where processing takes place for national security purposes. In each case, the controller or processor is required to put in place compensatory appropriate safeguards or security measures, as the case may be.

Part 3: Law Enforcement processing

Chapter 1: Scope and definitions

Clause 27: Processing to which this Part applies

165 This clause sets out the scope of the processing in respect of which the provisions in Part 3 of the Bill apply. The provisions of the LED and therefore of this Part are designed to be technology neutral. Accordingly the provisions cover the processing of personal data by computer systems or paper based structured filing systems (see definition in clause 2(7)). A structured filing system is one containing records relating to individuals that are held in a sufficiently systematic, structured way as to allow ready access to specific information about those individuals. Files which are not structured according to specific criteria do not fall within the scope of this Part.

Clauses 28 to 31: Definitions

166 These clauses and Schedule define terms used in Part 3. There are also additional definitions in clauses 2 and 184 which are relevant to the Bill as a whole. The definition of “personal data” in clause 2(2) is such that anonymised data falls outside the provisions of this Part as does data in relation to an individual who has died.

167 Schedule 7 specifies competent authorities. The list includes UK Government departments and ministers, chief officers of police, non-policing law enforcement agencies, prosecutorial agencies, other criminal justice agencies and other office holders or organisations who carry out activities in connection with law enforcement. A number of public organisations responsible for the investigation or prosecution of criminal offences or the execution of criminal penalties, are not legal entities in their own right. For example, HM Courts and Tribunals Service and HM Prison Service are executive agencies of the Ministry of Justice and, as such, would be caught by the entry at paragraph 1 of Schedule 7 in respect of ministerial Government departments. The entry in respect of UK Government departments only covers those departments which have functions in respect of particular categories of crime, for example the Department for Work and Pensions in relation to benefit fraud or the Home

Office in relation to immigration offences. Where a UK Government department or Scottish Ministers do not have responsibilities which involve the processing of personal data for law enforcement purposes, the entries in respect of Government Departments and Scottish Ministers will not impose obligations on those Departments or Ministers under this Part.

- 168 The list of competent authorities in Schedule 7 only covers the principal police and other criminal justice agencies in the UK which will, as part of their functions, process personal data for law enforcement purposes and are therefore subject to the provisions of this Part. Clause 27(1)(b) provides for a catch-all provision to capture other persons (that is, office holders or organisations) exercising statutory functions for a law enforcement purpose, for example local authorities when prosecuting trading standards offences or the Environment Agency when prosecuting environmental offences. It does not, however, apply to a person undertaking a private prosecution. The intelligence agencies are expressly excluded from the definition of a competent authority as there is a potential overlap between their functions and the catch-all provision (for example, under section 1(4) of the Security Service Act 1989, the Security Service has a function of supporting police forces and other law enforcement agencies in the prevention and detection of serious crime). The processing of personal data by the intelligence services is governed by the provisions in Part 4 of the Bill.
- 169 Clause 28(3) enables the list of competent authorities in Schedule 7 to be amended by regulations. This regulation-making power will enable the Schedule to be updated to take account of changes in the name of a listed office or organisation (in such a case the negative procedure applies), the abolition of an existing office or organisation (or a change in its functions such that it no longer processes personal data for law enforcement purposes) or the creation of a new office or organisation which engages in the processing of personal data for law enforcement purposes (in the latter two cases the affirmative procedure applies).
- 170 The definition of “law enforcement purposes” in clause 29 sets the boundaries to which the data protection regime in Part 3 of the Bill applies. Not all processing of personal data by a competent authority will be for law enforcement purposes. Where such processing takes place for other purposes, for example, for HR purposes, this will be general processing and governed by either the GDPR or the applied GDPR regime (see Chapter 3 of Part 2).
- 171 Clause 30 provides for definitions of “controller” and “processor”. In relation to controllers, the term “joint controllers” is used where two or more persons act together to decide the purpose and manner of any data processing (see clause 56). For example, the Police National Computer is managed on behalf of all police forces in the UK with individual chief constables acting as joint data controllers. The controller and processor can be the same, will be split if a competent authority outsources functions to another person, in that event that other person will be the processor – the competent authority would remain the controller and retain legal responsibility for compliance with the provisions of this Part. Where an employee of a controller is processing data, he or she is not acting as a processor but on behalf of the controller, in effect, as the operational arm of a single legal entity. The definition of an employee in clause 31(2) ensures that, in this context, police officers and special constables (who are officer holders rather than employees) are treated as an extension of their chief officer.

Chapter 2: Principles

Clauses 32 to 40 and Schedule 8: Data protection principles

- 172 These clauses set out the six data protection principles governing the processing of personal data for law enforcement purposes. Controllers are under a general duty to comply with the data protection principles (clause 32(3)).

- 173 The first principle (clause 33) is that processing must be lawful and fair. In contrast to the first data protection principle under the GDPR (see Article 5(1)(a)) there is no requirement for data to be processed in a transparent matter. This omission reflects the fact that there will be circumstances in which a law enforcement agency will need to neither confirm nor deny that it processes personal data in respect of a particular individual as to do so may reveal operationally sensitive or potentially damaging information that could, for example, prejudice an ongoing criminal investigation. “Lawful” processing means authorised by either statute or common law. For example, Part 5 of the Police and Criminal Evidence Act 1984 (which applies to England and Wales) confers statutory authority for the taking and retention of DNA and fingerprints, while the [Domestic Violence Disclosure Scheme](#) relies on the police’s common law powers to disclose information where it is necessary to do so to prevent crime.
- 174 The requirement to process data fairly does not in itself prevent law-enforcement authorities from carrying out activities, such as covert investigations or video surveillance. Such activities can be done for 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, as long as they are in accordance with the law (for example, covert surveillance carried out under Part 2 of the Regulation of Investigatory Powers Act 2000) and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned. The data protection principle of fair processing is a distinct notion from the right to a fair trial as defined in Article 6 of the ECHR.
- 175 Article 10 of the LED generally prohibits the processing of “special categories of personal data” unless specific circumstances apply.
- 176 Clause 33 uses the term “sensitive processing” (as defined in subsection (8)) to refer to such “special categories of personal data”. Subsections (4) and (5) specify the two circumstances when sensitive processing may take place for law enforcement purposes, namely when the data subject has consented or where the processing is for one or more of the purposes specified in Schedule 8. As an additional safeguard, in each case, the controller must have an appropriate policy in place. Clause 40 makes further provision in respect of such appropriate policies in respect of sensitive processing.
- 177 The second principle (clause 34) requires personal data to be processed for specific, explicit and legitimate law enforcement purposes, namely for one or more of the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security. The personal data is permitted to be processed for a different law enforcement purpose than that initially processed for so long as it is a lawful purpose, proportionate and necessary. So, for example, the Crown Prosecution Service could process personal data for the purpose of the prosecution of criminal offences, that had an initial processing purpose of the preventing a criminal offence.
- 178 The third principle (clause 35) requires that personal data to be adequate and relevant and not excessive for the purposes for which it is processed. The term “adequate, relevant and not excessive” is also used (undefined) in the 1998 Act; Commissioner guidance provides that in practice this term means that controllers should ensure that:
- they hold personal data about an individual that is sufficient for the purpose they are holding it for in relation to that individual; and
 - they do not hold more information than is needed for that purpose.

179 The fourth principle (clause 36) requires personal data held by a controller to be accurate and kept up to date. In the law enforcement context, the principle of accuracy of data must take account of the circumstances in which data is being processed. It is accepted that, for example, statements by victims and witnesses containing personal data will be based on the subjective perceptions of the person making the statement. Such statements are not always verifiable and are subject to challenge during the legal process. In such cases, the requirement for accuracy would not apply to the content of the statement but to the fact that a specific statement has been made. Clause 36(2) recognises the distinction between personal data based on facts (for example, the details relating to an individual's conviction for an offence) and data based on personal assessments, such as a witness statement. The requirement to keep personal data up to date must also be viewed in this context. If an individual's conviction is overturned on appeal, police records must be amended to reflect that fact. However, this principle would not require the retrospective alteration of a witness statement which the appellate court found to be unreliable.

180 The fifth principle (clause 37) requires that personal data be kept no longer than is necessary. To comply with this principle, data controllers should establish time limits for erasure, or for periodic review. As with the 1998 Act, this clause does not specify minimum or maximum periods for the retention of data. In practice, to comply with the fifth principle, data controllers should review the length of time they retain personal data; consider the law enforcement purpose or purposes they hold information for in deciding whether, and if so for how long, to retain it; securely delete information that is no longer needed for law enforcement purposes; and update, archive or securely delete information that goes out of date. The retention of certain information for law enforcement purposes is governed by statutory rules. For example, in England and Wales, Part 5 of the Police and Criminal Evidence Act 1984 makes provision for the retention of fingerprints and DNA profiles. The retention periods vary depending on whether or not an individual has a conviction for an offence, for example, in the case of an adult convicted of a recordable offence his or her fingerprints and DNA profile may be retained indefinitely. The College of Policing's [Management of Police Information](#) provides a framework for the review, retention or disposal of the generality of information held by police forces in England and Wales for law enforcement purposes.

181 The sixth principle (clause 38) requires personal data to be processed in a secure manner. The Commissioner's guidance stipulates that, in practice, this means that controllers must have appropriate security to prevent the personal data they hold being accidentally or deliberately compromised. In particular, controller will need to:

- design and organise their security to fit the nature of the personal data they hold and the harm that may result from a security breach;
- be clear about who in their organisation is responsible for ensuring information security;
- make sure they have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

182 Clause 39 makes provision for safeguards where the processing of personal data for law enforcement purposes is necessary for archiving, research or statistical reasons. This may include anonymising the data.

Chapter 3: Rights of the Data Subject

Clause 41: Overview and scope

183 This Chapter specifies the rights of data subjects under Part 3 and the obligations on controllers to facilitate the exercise of those rights. The relevant rights are: the right to access to information about the processing of personal data relating to the data subject; the right to rectification of inaccurate data; the right to the erasure of personal data where the processing of such data would infringe the data protection principles or to restrict the processing of such data. Subsections (3) and (4) disapply the subject access rights and the rights to rectification, erasure and restriction of processing in relation to the processing of relevant personal data in the course of a criminal investigation or criminal proceedings. This is because, in such cases, defendants will have access to such data through alternative routes, for example, in England and Wales under the disclosure provisions in the Criminal Procedure and Investigations Act 1996.

Clause 42: Information: controller's general duties

- 184 This clause imposes general duties on controllers in respect of the provision of information. Subsection (1) sets out a minimum list of information that must be available to data subjects. Such generic information may be provided through a controller's website or supporting literature. The Commissioner has published a code of practice on communicating privacy information to individuals.
- 185 Subsection (2) sets out additional information which a controller must provide to a data subject to enable the data subject to exercise his or her subject access rights.
- 186 The right to the information specified in subsection (2) is a qualified right. Subsection (4) sets out various grounds on which a controller may restrict the provision of information under subsection (2). This recognises, for example, that the disclosure of such information could compromise an ongoing police investigation or compromise sensitive operational techniques or capabilities.

Clause 43: Right of access by the data subject

- 187 This clause sets out the right of access accorded to data subjects and the information that should be disclosed on request so that the data subject is aware of, and can verify the lawfulness of the processing. Securing such access would then enable a data subject, if necessary, to exercise the other rights provided for in this Chapter, namely the rights to rectification, erasure or restriction on processing. Controllers must respond to subject access requests without undue delay and, in any event, within one month (compared with 40 days under the 1998 Act).
- 188 As with the previous clause, the subject access rights conferred by this clause are not absolute and subsection (4) provides for the same grounds on which a subject access request may be refused, whether wholly or in part. Operationally, law enforcement bodies may receive a subject access request from an individual who, unknown to them, is under investigation. If this investigation forms all of the information held about the data subject, then informing them that their rights have been restricted for the purpose of "avoiding prejudice to the investigation, detection, investigation or prosecution of criminal offences or the execution of criminal penalties" could potentially alert the data subject to the existence of the investigation and could lead to the investigation being compromised. Instead, the data subject would receive a "Neither Confirm nor Deny" response. As a safeguard, the controller must record what they have done and make it available to the Commissioner (if requested).

Clauses 44 to 46: Data subject's rights to rectification or erasure etc

- 189 These clauses enable a data subject to ask for data to be corrected, erased or for processing of that data to be restricted. The data subject is allowed to challenge the processing of the data directly to the controller. Correction can include adding to incomplete personal data. The right to rectification applies, in particular, to matters of fact. For example, there may be inaccuracies in the details of a criminal conviction held on the Police National Computer - an individual may receive a copy of their criminal record and request that an incorrect entry for Grievous Bodily Harm be corrected to Actual Bodily Harm, or vice versa, to reflect the correct conviction. The right to rectification would not apply, for example, to the content of a witness statement. In such a case, it would be more appropriate to restrict the processing of the personal data contained in the statement so that it was only used in connection with relevant criminal proceeding. An underlying assumption would be to restrict data processing rather than to erase it in cases where erasure can affect the interests of the data subject or a third party. Restricted data should be processed only for the purpose which prevented its erasure.
- 190 Restrictions on the processing of data may be given effect by moving the data to another system, for example for archiving purposes, or making it unavailable. The fact that the processing of the personal data is restricted should be indicated on the system, for example, through flagging.
- 191 Where a data subject's request for rectification or erasure has been refused, the data subject must be informed of the reasons for the refusal. Again, it is open to a controller not to provide such reasons where, to do so, is necessary and proportionate for the purposes specified in subsection (3) of clause 46.
- 192 Where this exemption has been exercised, the data subject may lodge a complaint with the Commissioner. Clauses 156 and 157 make further provision in respect of complaints by data subjects.
- 193 If a controller has rectified, erased or restricted processing for certain data, there is a duty on the controller to inform the competent authority from where the data originated (if different) and to alert any recipients of the data. This is particularly important if data has been transferred internationally (see Chapter 5 of Part 3 for more detail on international transfers).

Clauses 47 and 48: Automated individual decision-making

- 194 These clauses establish the right for individuals not to be subject to decisions based solely on automated processing and resulting in adverse legal effects or any other significant impacts. If controllers are using automated processing, suitable safeguards should be in place, including where appropriate, informing the data subject what has taken place and his or her right to request human intervention in the processing or decision, to obtain an explanation of the decision reached or to challenge the decision. The clause places a duty on the controller to consider any request for a review of an automated decision.
- 195 In practice, currently automated processing that leads to an adverse outcome is rarely used in the law enforcement context and is unlikely to have any operational implications.

Clauses 49 to 52: Supplementary

- 196 These clauses make supplementary provisions about the exercise of data subjects' rights. These are broadly in line with the provisions of the 1998 Act, in that information should be made available in the format it was requested (where practicable), but any means are permissible and responses for information can be delayed whilst the identity of the requester is verified. However the key distinction here between the 1998 Act and the new regime is the requirement to respond to a subject access request free of charge (the 1998 Act currently permits data controllers to charge an administration fee of up to £10).

197 Clause 51, however, makes special provision for subject access requests that are “manifestly unfounded or excessive”. This may include requests that are repetitious, are malicious in intent or where they represent an abuse of the rights to access, for example by providing false or misleading information. Similarly data subjects might attempt to use the right of subject access as a means to harass law enforcement bodies with no real purpose other than to cause disruption to the organisation. This can be in the form of repeated requests over a relatively short period of time or extending over several years. In these circumstances the controller can charge a reasonable fee (subject to any prescribed maximum) to act on the request or can refuse the request entirely. The burden is on the controller to demonstrate that the request is manifestly unfounded or excessive.

Chapter 4: Controller and processor

Clause 53: Overview and scope

198 This overview clause is self-explanatory.

Clauses 54 to 63: General obligations

199 This Chapter provides for obligations on controllers and processors. Clauses 54 and 55 impose general obligations on controllers to take appropriate technical and organisational measures to ensure that the requirements of Part 3 are complied with. In order to demonstrate compliance with Part 3, controllers should adopt internal policies and implement measures which adhere to the principle of data protection by design and data protection by default. Overall the measures implemented need to be proportionate to the processing activities, but this is not just an economic consideration; measures should adhere to the data principles and the outcome of any completed data protection impact assessment (see clause 62).

200 The intention is to ensure that data protection is mainstreamed in processing operations, particularly in the planning of new proposals or projects, although equally relevant for existing processing operations. Instead of data protection input emerging once plans are in place or the processing has begun, this places an obligation on the controller to put in place appropriate technical and organisational measures to implement the data protection principles. This aims to ensure controllers only process personal data which is necessary for the specific purposes of the processing and the processing reflects and complies with the principles. Methods of processing such as pseudonymisation may assist in meeting these obligations. The purpose is not to place undue burdens on the controller, however an assessment of available technology, cost, type of data and any risks (such as damage to reputation) linked to processing must be considered when applying appropriate technical and organisational safeguards.

201 Clause 56 establishes the responsibilities for joint controllers. Where two or more controllers jointly determine the purposes and means of processing they are considered joint controllers. To ensure the protection of the rights of data subjects any arrangements in relation to joint controllers must ensure there is unambiguous apportionment of the responsibilities as set out in Part 3. Controllers should determine their obligations by means of a transparent arrangement between them, for example, under the terms of a collaboration agreement between police forces in England and Wales made under section 22A of the Police Act 1996.

202 Clause 57 sets out the requirements on processors. As above, the processor also needs to implement the technical and organisational measures necessary to ensure it is compliant with the law. It is vital that the controller is satisfied that the processor can and does implement these measures. A processor must not engage with another processor without authorisation from the controller, this means that specific permission from the controller must be sought before engaging any sub-processors or contractors.

- 203 There is also a requirement to ensure that the service provided by a processor be governed by a contract or other legal act, which is binding on the processor with regard to the controller. This provision specifies a number of provisions that will ensure the lawfulness of the processing that must be included in the contract or other legal instrument, including a duty to confidentiality.
- 204 Overall the controller may need, if requested, to demonstrate its own processing or that done on its behalf by a processor is compliant with requirements. Any arrangement between the controller and processor will need to reflect this requirement.
- 205 To that end, clause 59 specifies what records should be kept by controllers and processors, these records need to be made available to the Commissioner on request, and are a means of demonstrating compliance with the law. The processing of personal data in non-automated processing systems (that is, paper based filing) also needs to be appropriately monitored by controllers and processors, and there should be in place methods of demonstrating lawfulness of processing, and data security and integrity. This may be through logs or other forms of records.
- 206 Clause 60 imposes logging requirements. Such requirements are not imposed by the 1998 Act. The purpose of the requirement is to enable a controller to monitor and audit data processing internally. The purposes for which logs may be used, including self-monitoring, are set out in subsection (4)(b). Self-monitoring includes internal disciplinary proceedings with a competent authority. The Independent Police Complaints Commission have published guidance on the recording of police complaints and an example of a category of complaint that this may be relevant to is: category Z - Improper access and/or disclosure of information. If, for example, an officer or member of police staff was suspected of inappropriately accessing the Police National Computer to check on neighbours, family or friends, the logging should show what was available to them at the time which would assist the investigation possibly leading to criminal or disciplinary action and possible dismissal.
- 207 Many automated systems have existing logging capabilities; however there is a requirement within the clause to log erasure of personal data, as well as collection, alteration, consultation, etc. Logs of erasure should not reference the data itself – there is no need to retain a record of what was erased (as that too would also be a record), rather, the log should be able to specify that an item of data was erased on a specific date by a specific person. Article 63(2) of the LED provides for a transitional period in respect of the logging requirements for automated processing systems set up before 6 May 2016; in such cases the requirements of Article 25(1), as transposed by clause 60, must apply by 6 May 2023.
- 208 Clause 62 places data protection impact assessments (“DPIA”) on a statutory footing. The Commissioner has issued a code of practice in respect of the existing, non-statutory, Privacy Impact Assessments. The assessments should highlight and address privacy issues where a controller intends to process personal data in a way which could result in a high risk to data subject rights and freedoms. Impact assessments should cover relevant systems and processes (not individual cases) and should consider the human rights issues of processing the data. In policing, the use of Privacy Impact Assessments has increased in recent years with examples such as in the introduction of Body Worn Video and development of the Child Abuse Image Database. This provision requires DPIAs at the outset and for them to be mainstreamed into the project planning lifecycle. The content of the DPIA must include the matters specified in subsection (3).
- 209 Where an impact assessment has indicated there is a high risk associated with the processing there is a new requirement for a controller, or where appropriate a processor, to consult with the Commissioner prior to conducting that processing operation. The Commissioner may

provide written advice as to how to conduct the processing or implement mitigating measures.

Clause 64 and 65: Obligations relating to security

210 This clause sets out the security obligations on the controller, and where necessary the processor, in both manual and automated processing. The essence of the requirement is to ensure that data is protected according to the risk. Risks will need to be evaluated and appropriate measures implemented, for example, this might include encryption as this would mitigate the effects of any breach, or specific levels of security clearance for staff processing the data.

211 A personal data breach could lead to a loss of control over data, limitation of rights, reputational damage and other social or economic disadvantages. Therefore, in the event of a data breach whereby there is a significant risk to the rights and freedoms of the individual, the controller is obliged to inform the Commissioner without undue delay, and where feasible, within 72 hours and give details as to how they are mitigating that risk.

Clause 66: Communication of a personal data breach to the data subject

212 When there is a high risk to the rights and freedoms of an individual as a result of a data breach the data subject(s) should also be notified of the data breach in good time so they may take the necessary precautions to protect themselves. The communication should be made as soon as possible relative to the risk, for example if there is an immediate risk of damage a quick response to data subjects would be advisable (this can be a mass communication if applicable). Given the nature of the data being processed, this clause enables controllers to withhold notice of a data breach in circumstances where notifying a data subject would reveal the existence of the data.

Clauses 67 to 69: Data protection officers

213 These clauses provide for the appointment and the tasks of data protection officers (“DPO”). There is no current requirement under the 1998 Act for controllers to appoint a DPO, but some controllers may already have an individual who performs a similar role. An individual designated as a DPO must have the appropriate skills and training for the role. The level of knowledge should be commensurate to the types of data processing the controller carries out; some types of processing will require a more bespoke skill set than others, a DPO for the police, for example, will require significant knowledge of the numerous systems that are operated in policing and the legal context for them. Depending on the size and function of the organisation, the DPO could be part-time or full-time, or one DPO could be appointed to work on behalf of several controllers (police forces for example could have one DPO per region as opposed to one per force). Irrespective, the DPO will need to be suitably senior and resourced to be able to undertake his or her duties.

214 Clause 69 sets out a number of specific tasks to be discharged by a DPO, but overall the role is to assist the controller and employees actually involved in the data processing in how to make sure operations are compliant with the law and with data protection obligations. DPOs must be able to perform their duties independently.

Chapter 5: Transfers of personal data to third countries etc

Clause 70: Overview and interpretation

215 The transfer of personal data to a third country (as defined in subsection (2)) or to an international organisation should only take place if necessary for a law enforcement purpose, and when the controller in the third country or international organisation carries out functions comparable to those of a competent authority within the meaning of clause 28.

216 Where personal data is transferred from the UK to controllers, processors or other recipients in third countries or international organisations, the level of protection of individuals provided for in the UK by Part 3 should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers or processors in the same, or in another, third country or international organisation.

Clauses 71 to 74: General principles for transfers

217 Clause 71 requires any transfers of data to satisfy the conditions set out in subsections (2) to (4). Condition two relates to the standards of data protection in the recipient third country or international organisation. The European Commission will decide, with effect for the entire EU, that certain third countries, a territory or one or more specified sectors within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the EU as regards the third countries or international organisations which are considered to provide such a level of protection. In such cases, transfers of personal data to those countries should be able to take place without the need to obtain any specific authorisation, except where another Member State from which the data were obtained has to give its authorisation to the transfer. To date, the Commission has adopted 12 adequacy decisions with: Andorra, Argentina, Canada (for transfers to commercial organisations who are subject to the Canadian Personal information Protection and electronic Documents Act), the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and the United States (for certified companies).

218 The European Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation, no longer ensures an adequate level of data protection. Consequently, the transfer of personal data to that third country or international organisation should be prohibited unless the requirements of clause 73 or 74, which govern transfers based on appropriate safeguards and specific circumstances, are fulfilled.

219 Transfers not based on such an adequacy decision are allowed only where appropriate safeguards have been provided in a legally binding instrument (for example, a bilateral agreement between the UK and a third country) which ensures the protection of personal data or where the controller has assessed all the circumstances surrounding transfers of that type of data and, on the basis of that assessment, considers that appropriate safeguards with regard to the protection of personal data exist. Controllers are able to take into account cooperation agreements concluded between Europol or Eurojust and third countries which allow for the exchange of personal data when carrying out the assessment of all the circumstances surrounding the data transfer. A controller may also take into account the fact that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition, a controller should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment. While those conditions could be considered to be appropriate safeguards allowing the transfer of data, a controller should be able to require additional safeguards.

220 Where no adequacy decision or appropriate safeguards exist, clause 74 provides that a transfer or a category of transfers could take place only in specific situations, if necessary to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject; for the prevention of an immediate and serious threat to the public security of a Member State or a third country; in an individual case for 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; or in an individual case a legal purpose, including the establishment, exercise or

defence of legal claims. Such transfers should be documented and should be made available to the supervisory authority on request in order to monitor the lawfulness of the transfer.

Clause 75: Transfers of personal data to persons other than relevant authorities

221 In specific individual cases, the regular procedures requiring transfer of personal data to a relevant authority in a third country may be ineffective or inappropriate, in particular because the transfer could not be carried out in a timely manner, or because that authority in the third country does not respect the rule of law or international human rights norms and standards, so that a competent authority could decide to transfer personal data directly to recipients established in those third countries. This may be the case where there is an urgent need to transfer personal data to save the life of a person who is in danger of becoming a victim of a criminal offence or in the interest of preventing an imminent perpetration of a crime, including terrorism.

222 Such a transfer between competent authorities and recipients established in third countries should take place only in specific individual cases, and subject to the specific provisions of this Part of the Bill. These provisions should not be considered to be derogations from any existing bilateral or multilateral international agreements in the field of judicial cooperation in criminal matters and police cooperation. Those rules should apply in addition to the other rules in Part 3 and with particular regard to the lawfulness of processing.

Clause 76: Subsequent transfers

223 Where personal data is transferred from the UK to third countries or international organisations, any subsequent transfer should, in principle, take place only after the competent authority from which the data was obtained has given its authorisation to the transfer. Onward transfers of personal data should be subject to prior authorisation by the competent authority that carried out the original transfer (the original transfer should provide the recipient with any specific handling conditions). When deciding on a request for the authorisation of an onward transfer, the competent authority that carried out the original transfer should take due account of all relevant factors, including the seriousness of the criminal offence, the specific conditions subject to which, and the purpose for which, the data was originally transferred, the nature and conditions of the execution of the criminal penalty, and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred. The competent authority that carried out the original transfer should also be able to subject the onward transfer to specific conditions. Such specific conditions can be described, for example, in handling codes.

Chapter 6: Supplementary

Clause 77: National security: certificates by the Minister

224 This clause provides that a Minister of the Crown (as defined in subsection (12)) may certify that, for the purposes of clause 42(4), 43(4), 46(3) and 66(7) a restriction is necessary and proportionate to protect national security. Subsection (3) provides that such a certificate is to be taken as conclusive evidence that the restriction (both specific and general) is required. A certificate issued by a Minister of the Crown is a means of giving a controller legal certainty as to the application of a restriction. This replicates analogous provisions in section 28 of the 1998 Act.

225 Any person directly affected by the issuing of any certificate may appeal to the tribunal to judicially review the decision to issue the certificate (subsections (5) and (6)). A party to proceedings may also challenge the application of a certificate to the processing of particular personal data (subsections (7) to (9)).

Clause 78: Special processing restrictions

226 This clause provides that where any national restrictions (other than those provided for by or under this Bill) apply to the processing of personal data, such restrictions must also be applied where such personal data is shared with a recipient in another EU Member State or with an organization established under the judicial co-operation or police co-operation provisions of the TFEU.

Clause 79: Reporting of infringements

227 This clause requires controllers to put in place procedures to encourage confidential reporting of infringements of the provisions of Part 3. The intention here is that controllers should have internal procedures to promote the organisation's compliance with the provisions in Part 3 by encouraging staff to self-report known or suspected infringements without fear of them being victimised, including through the taking of disciplinary action against them. Such procedures should, amongst other things, raise employees' awareness of the whistle-blowing provisions in relevant employment rights legislation. Part 4A of the Employment Rights Act 1996, which applies to England and Wales and Scotland (there is equivalent legislation in Northern Ireland), provides for certain protections for workers who make a disclosure which they reasonably believe and it is in the public interest that one or more specified matters is either happening, has taken place, or is likely to happen in future. The specified matters include a criminal offence and a breach of a legal obligation. Workers who 'blow the whistle' on wrongdoing in the workplace can claim unfair dismissal if they are dismissed or victimised for doing so.

Part 4: Intelligence services processing

Chapter 1: Scope and definitions

Clauses 80 to 82: Processing to which this Part applies and definitions

228 Clause 80 applies the provisions in Part 4 of the Bill to personal data controlled by an intelligence service (the Security Service, Secret Intelligence Service and Government Communications Headquarters).

229 The intelligence services process data in accordance with their functions, which are set out in the Security Service Act 1989 and the Intelligence Services Act 1994. Those functions are:

- The Security Service:
 - the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.
 - safeguarding the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands.
 - acting in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection of serious crime.
- The Secret Intelligence Service:
 - to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and
 - to perform other tasks relating to the actions or intentions of such persons.

These functions are exercisable only —

- in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or
 - in the interests of the economic well-being of the United Kingdom; or
 - in support of the prevention or detection of serious crime.
- Government Communications Headquarters:
 - a) to monitor, make use of or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material; and
 - b) to provide advice and assistance about —
 - i. languages, including terminology used for technical matters, and
 - ii. cryptography and other matters relating to the protection of information and other material,
- to the armed forces of the Crown, to Her Majesty's Government in the United Kingdom or to a Northern Ireland Department or, in such cases as it considers appropriate, to other organisations or persons, or to the general public, in the United Kingdom or elsewhere.

The functions referred to in paragraph (a) are exercisable only —

- in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or
- in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or
- in support of the prevention or detection of serious crime.

230 Clause 81 defines “processor” and “controller” for the purposes of intelligence service processing under Part 4.

231 An intelligence service is a controller when, alone or jointly with others, it determines the purposes and means of processing of personal data. A processor is any person who processes personal data on behalf of the controller.

232 When personal data is processed only for purposes required by legislation, and by means stipulated by that legislation, the person who has the obligation to process the data is the controller.

233 If a controller outsources processing functions to another person or organisation then that other person or organisation will be a processor. The data processor acts on behalf of the data controller, and follows their direction. Employees of the controller are not considered data processors because they are part of the single legal entity that is the controller.

234 The provisions of this Part are technology neutral, covering the processing of personal data by computer systems or paper based structured filing systems (see definition in clause 2(7)). A structured filing system is one containing records relating to individuals held in a sufficiently systematic, structured way as to allow ready access to specific information about those individuals. Files which are not structured according to specific criteria do not fall within the scope of this Part.

235 Clause 82 defines other expressions used in this Part.

Chapter 2: Principles

Clauses 83 to 89 and Schedules 9 and 10: Data protection principles

- 236 These clauses set out the six data protection principles governing the processing of personal data by intelligence services, and make further provision about the application of those principles.
- 237 The first principle (clause 84) is that processing must be lawful, fair and transparent. The conditions under which processing is lawful are set out in Schedule 9, and include where the data subject has given their consent, where the processing is necessary for compliance with a legal obligation, where the processing is necessary for the statutory function of an intelligence service or where the processing is necessary for the administration of justice. The criteria for sensitive processing (defined in clause 84(7)) are stricter and are set out in Schedule 10. Clause 84(3) confers a regulation-making power (subject to the affirmative procedure) on the Secretary of State to add to, vary or omit conditions in Schedule 10.
- 238 The requirement to process data fairly does not in itself prevent intelligence services from carrying out activities such as covert surveillance. Such activities would be regarded as fair and lawful if they comply with the requirements of the Human Rights Act 1998 (for example, where interference with privacy is permissible because it is both necessary and proportionate), the purposes and functions and disclosure gateways specified in the Security Service Act 1989 and Intelligence Services Act 1994 (as appropriate) or any other relevant legislation (for example, the Regulation of Investigatory Powers Act 2000 or the Investigatory Powers Act 2016).
- 239 The principle of transparency requires data controllers to be clear and open with data subjects about how information about them will be used. This could be achieved, for example, by providing generic information on a website about the identity of the controller, the purposes of the processing undertaken by the controller, rights available to data subjects and other information as specified.
- 240 The second principle (clause 85) requires personal data to be collected for specific, explicit and legitimate purposes. The statutory functions of the intelligence services are set out in the Security Service Act 1989 (for MI5) and the Intelligence Services Act 1994 (for MI6 and GCHQ). Personal data collected for one purpose may be processed for another. The use for that other purpose, however, must also be lawful, proportionate and necessary. So, for example, personal data collected by the Security Service for the purpose of safeguarding national security could be processed further for the purpose of the prevention or detection of serious criminal offences, for instance by alerting the relevant law enforcement agency to intelligence suggesting a subject of interest is in possession of a firearm.
- 241 The third principle (clause 86) requires that personal data undergoing processing by controllers be adequate and relevant and not excessive for the purposes for which it is processed. That means that a controller:
- holds personal data about an individual that is sufficient for the purpose in question; and
 - does not hold more information than is needed for that purpose.
- 242 The fourth principle (clause 87) requires personal data undergoing processing to be accurate and, where necessary, kept up to date. The accuracy of personal data held by a controller under Part 4 might not always be a straightforward question of fact in cases where it amounts to an intelligence officer's assessment which is based on underlying information which is partial or incomplete.

243 The fifth principle (clause 88) requires that personal data undergoing processing be kept no longer than is necessary. To comply with this principle, data controllers should establish time limits for erasure, or for periodic review. As with the 1998 Act, this clause does not specify minimum or maximum periods for the retention of data. In practice, to comply with the fifth principle, data controllers should review the length of time they retain personal data; consider the purpose or purposes they hold information for in deciding whether, and if so for how long, to retain it, updating or archiving information and securely deleting information that is no longer needed for those purposes.

244 The retention of certain information by intelligence services is governed by statutory rules. For example, the Investigatory Powers Act 2016 requires the retention and examination of a bulk personal dataset by an intelligence service to be authorised by a warrant issued by a Secretary of State and approved by a Judicial Commissioner.

245 The sixth principle (clause 89) requires personal data to be processed in a secure manner. The current Commissioner guidance stipulates that, in practice, this means that controllers must have appropriate security to prevent the personal data they hold being accidentally or deliberately compromised. In particular, controllers will need to:

- design and organise their security to fit the nature of the personal data they hold and the harm that may result from a security breach;
- be clear about who in their organisation is responsible for ensuring information security;
- make sure they have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

Chapter 3: Rights of data subjects

Clause 90: Overview

246 This Chapter specifies the rights of data subjects under Part 4 and the obligations on controllers to facilitate the exercise of those rights. The rights are: the right to information about the processing of personal data by the controller; the right of access to information processed relating to the data subject; rights in relation to automated processing; rights to object to processing; the right to rectification, erasure or restriction of personal data.

Clause 91: Right to information

247 A controller is required to provide a data subject with specified information about the processing of personal data by the controller. This includes the identity and contact details of the controller, the purposes and legal basis for which personal data may be processed, and information about the data being processed. Such information may be made generally available, for example, through the controller's website.

248 This obligation does not apply if the data subject already has the relevant information. Nor does it apply where data is collected from a third party source (that is, not from the data subject), if the processing is authorised under an enactment, or if providing the information is impossible or would involve disproportionate effort.

Clauses 92 and 93: Right of access

249 These clauses set out the right of access accorded to data subjects and the information that should be disclosed on request so that the data subject is aware of, and can verify the lawfulness of the processing. Securing such access would then enable a data subject, if

necessary, to exercise the other rights provided for in this Chapter, namely the rights to rectification and erasure. Controllers must respond to subject access requests promptly and, in any event, within one month (or such longer period, not exceeding three months, as is specified in regulations made by the Secretary of State). In contrast to the GDPR and the provisions in Part 3 of the Bill, under these provisions a data controller may, as now, charge a reasonable fee before responding to subject access requests.

250 Clause 92(6) and 93(5) provide for situations where the personal data which would be disclosed following the right to information, also constitutes the personal data of another person. In such cases the data controller may restrict the provision of this data, unless the other party has consented to the disclosure or can be rendered unidentifiable.

251 Clause 93 describes how the controller must provide a copy of personal data to a data subject, and the circumstances under which a controller may decline to respond to a subject access request where it duplicates a previous one.

Clauses 94 to 96: Rights related to decision-making

252 Clauses 94 and 95 provide for a general right for individuals not to be subject to decisions based solely on automated processing and resulting in adverse legal effects or any other significant impacts. It allows for such decisions to be made in certain circumstances, such as when required or authorised by an enactment. In the case of an automated decision being taken when required or authorised by an enactment, the data controller must notify the data subject that the decision has been made. In these circumstances, the data subject has a right to ask the controller to reconsider the decision or to take a new decision not based solely on automated processing (clause 95).

253 Clause 96 confers on data subjects a right to obtain the reasoning underlying the processing of data which results in a decision being applied to the data subject (whether or not as a result of automated decision-making).

Clause 97: Right to object to processing

254 This clause allows a data subject to require the controller not to process the subject's personal data on the grounds that the processing is an unwarranted interference with their interests or rights. Upon receipt of such a request, a controller has 21 days to comply or respond with their reasons for not complying. If the controller does not comply with the request, the data subject may apply to the High Court (or, in Scotland, the Court of Session), which may order the controller to take steps in complying with the request (so far as the court considers is necessary).

Clause 98: Right to rectification or erasure

255 This clause enables a data subject to ask for data to be corrected or erased. The data subject may make an application to the High Court (or, in Scotland the Court of Session) for an order requiring such rectification or erasure. The High Court, or Court of Session, is considered to be the appropriate forum to consider cases in respect of the intelligence services.

256 Correction can include adding to incomplete personal data and applies, in particular, to matters of fact. For example, there may be inaccuracies in the details of a criminal conviction or address history. However, the right to rectification would not apply, for example, to the content of a witness statement.

257 This clause also enables a court to order the controller to restrict processing of data, rather than requiring correction or deletion. Restrictions on the processing of data may be given effect by moving the data to another system, for example archiving the data, or making it unavailable. The fact that the processing of the personal data is restricted should be indicated

on the system, for example, through flagging. Restricted data should be processed only for the purpose(s) which prevented its erasure.

Chapter 4: Controller and processor

Clause 99: Overview

258 This overview clause is self-explanatory.

Clauses 100 to 104: General obligations of controllers and processors

259 These clauses provide for obligations on data controllers and processors.

260 Clauses 100 and 101 impose general obligations on controllers to take appropriate technical and organisational measures to ensure that the requirements of Part 4 are complied with. In order to demonstrate compliance with Part 4, controllers should adopt appropriate technical and organisational measures which ensure that risks to the rights and freedoms of data subjects are minimised.

261 The intention is to ensure that data protection is central to processing operations, including in the planning of new proposals or projects. Instead of data protection being considered after plans are in place or after processing has begun, this places an obligation on the controller prior to processing to put in place appropriate technical and organisational measures to implement the data protection principles. This will ensure that controllers only process personal data which is necessary for the specific purposes of the processing and that the processing reflects and complies with the data protection principles. The purpose is not to place undue burdens on the controller, however an assessment of available technology, cost, type of data and any risks linked to processing must be considered when applying appropriate technical and organisational measures.

262 Clause 102 establishes the responsibilities for joint controllers. Where two or more controllers jointly determine the purposes and means of processing they are considered joint controllers. To ensure the protection of the rights of data subjects any arrangements in relation to joint controllers must ensure there is unambiguous apportionment of the responsibilities provided for in Part 4.

263 Clauses 103 provides that data controllers may only use data processors to process personal data on their behalf if the processor undertakes to implement appropriate measures to comply with the requirements of this Part, and to provide any information necessary to demonstrate that compliance. Data processors (and any person acting under the authority of a processor or controller) may only process personal data on instruction from the controller or to comply with a legal obligation (clause 104).

Clause 105: Security of processing

264 This clause sets out the security obligations on the controller, and where necessary the processor, in both manual and automated processing. The essence of the requirement is to ensure that data is protected according to the risk. Risks will need to be evaluated and appropriate measures implemented. These might include:

- record- or log-keeping to ensure access to and processing of the data can be audited;
- an ability to verify the integrity of stored data and restore it if it becomes corrupted;
- specific levels of security clearance for staff processing the data;
- restricting physical access to systems holding personal data;
- network security measures to prevent unauthorized access to electronic systems; or

- restrictions on access to data by staff who do not need to access to that element of the personal data held by the controller.

Clause 106: Communication of personal data breach

265 A personal data breach could cause serious harm to data subjects. Therefore, in the event of a data breach which seriously interferes with the rights and freedoms of an individual or individuals, this clause requires the controller to inform the Commissioner without undue delay. If the report is not made within 72 hours, when it is subsequently provided it must be accompanied by an explanation of the reasons for the delay.

266 The duty on a controller is disapplied (subsection (6)) where the personal data breach also constitutes a relevant error under section 231 of the Investigatory powers Act 2016. This is designed to avoid the double reporting of breaches. A relevant error under the Investigatory Powers Act means an error made by a public authority in complying with any requirement over which the Investigatory Powers Commissioner has oversight.

267 If a processor becomes aware of a personal data breach, they must notify the controller.

Chapter 5: Transfers of personal data outside the United Kingdom

Clause 107: Transfers of personal data outside the United Kingdom

268 This clause provides that the transfer of personal data to a country outside the United Kingdom or to an international organisation may only take place where the transfer is necessary and proportionate in accordance with the controller's statutory functions (see paragraph 218), or relevant provisions of the Security Service Act 1989 and the Intelligence Services Act 1994. Those provisions place the Director General, Chief and Director of the Security Service, Secret Intelligence Service and GCHQ respectively under a duty to ensure that there are arrangements for securing that no information is obtained by the relevant service except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or:

- In the case of the Security Service - for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings;
- In the case of the Secret Intelligence Service - in the interests of national security; for the purpose of the prevention or detection of serious crime; or for the purpose of any criminal proceedings; and
- In the case of GCHQ - for the purpose of any criminal proceedings.

Chapter 6: Exemptions

Clause 108 and 109: National security

269 Clause 108 creates an exemption from certain provisions in the Bill if that exemption is required for the purpose of safeguarding national security. The provisions from which there is an exemption are in Parts 4 to 6 of the Bill and include most of the data protection principles, the rights of data subjects, certain obligations on data controllers and processors, and various enforcement provisions. This exemption mirrors the provision in section 28 of the 1998 Act.

270 Clause 109 provides that, as now under the provisions of the 1998 Act, a Minister of the Crown (as defined in subsection (10)) may certify that an exemption for the purposes of safeguarding national security is required in respect of specified personal data or processing. Subsection (1) provides that such a certificate is to be taken as conclusive evidence of the exemption being required.

271 These provisions allow departure from requirements of the Bill where this is necessary to safeguard national security. For instance, they will exempt an intelligence service controller from having to reveal to a terrorist suspect subject to covert surveillance, that personal data relating to him or her is being processed.

272 A certificate issued by a Minister of the Crown is a means to give an intelligence service legal certainty that an exemption applies to the specified data processing. Any person directly affected by the issuing of any certificate may appeal to the tribunal to judicially review the decision to issue the certificate or, where the certificate identifies data by means of a general description, challenge the application of the certificate to specific data.

Clauses 110 and 111 and Schedule 11: Other exemptions

273 There are some other circumstances where the principles and rights established by the Bill may conflict with other public interests or individual rights. Clause 110 introduces Schedule 11, which provides for an exemption from certain provisions of the Bill for data processed for certain listed purposes, such as:

- information which is required in connection with legal proceedings;
- information which is legally privileged; or
- for the protection of the information rights of other data subjects.

274 Clause 111 provides for a power for the Secretary of State, by regulations (subject to the affirmative procedure) to create further exemptions from the provisions of Part 4. It also provides the power to amend or repeal any of the provisions in Schedule 11.

Part 5: The Information Commissioner

275 In this part references to the GDPR are to the GDPR read with Chapter 2 of Part 2 and include the applied GDPR read with Chapter 3 of Part 2; references to processing and personal data are to processing and personal data to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies.

Clause 112: The Information Commissioner

276 This clause makes provision for the continuing existence of the Commissioner and introduces Schedule 12 which makes provision about matters such as the status, capacity and appointment of the Commissioner.

Clause 113: General functions under the GDPR and safeguards

277 The Commissioner will continue to be the supervisory authority in the United Kingdom for the purposes of Article 51 of the GDPR.

278 In relation to the processing of personal data to which the GDPR applies, the Commissioner must advise Parliament and other bodies on legislative and other measures and may also issue opinions to those bodies on any issue relating to the protection of personal data.

279 The exercise of the Commissioner's functions conferred by Articles 57 and 58 of the GDPR is subject to safeguards provided for in the Act.

Clause 114: Other general functions

280 Subsection (1)(a) is a new provision for the Commissioner to be the supervisory authority for the purpose of Article 41 of the LED, which requires Member States to have a supervisory authority responsible for monitoring application of the Directive.

281 Subsection (1)(b) makes a provision for the Commissioner to continue to be the UK's designated authority for the purposes of Article 13 of the Convention. Clause 2 provides a definition of the Convention.

Clause 115: Competence in relation to courts etc

282 Article 55(3) of the GDPR provides that supervisory authorities cannot supervise processing operations of courts in their judicial capacity. Article 45(2) of the LED provides the same restriction.

283 This clause is a new provision which confirms this limited scope of the Commissioner's functions in relation to the processing of personal data by a judge or a court or tribunal.

Clause 116: Co-operation and mutual assistance

284 In line with the GDPR requirements, the Commissioner is required to co-operate with other supervisory authorities and with the Data Protection Board and the European Commission.

285 This clause sets out the Commissioner's functions regarding co-operation and mutual assistance with other supervisory authorities under the GDPR, LED and the Convention 108.

286 Schedule 14 to the Bill provides further details about the circumstances in which the Commissioner can exercise these functions. Part 1 concerns mutual assistance. Part 2 concerns co-operation between parties.

Clause 117: Inspection of personal data in accordance with international obligations

287 This clause is similar to section 54A of the 1998 Act, but rather than listing specific systems, the provision has been future-proofed to allow the Commissioner to inspect personal data held in any automated or structured system where the inspection is necessary to discharge an international obligation of the United Kingdom. Subsections (2) to (5) provide further provisions about when the power is exercisable.

288 Subsection (6) provides that it is an offence to obstruct such an inspection or to fail, without reasonable excuse, to give any assistance that may be required.

Clause 118: Further international role

289 This clause creates an obligation on the Commissioner to engage with third countries and international organisations. Subsection (1) It includes developing international cooperation mechanisms, international assistance in enforcement, engaging stakeholders in furthering cooperation and promoting the exchange and documentation, and practice relating to jurisdictional conflicts with third countries for the enforcement of legislation and protection of personal data.

290 Subsection (2) clarifies that this obligation under subsection (1) does not relate to processing regulated by the GDPR.

291 Subsection (3) requires the Commissioner to carry out data protection functions directed by the Secretary of State, enabling the UK to comply with international obligations.

292 Subsection (4) enables the Commissioner to provide assistance to an authority carrying out data protection functions under the law of a British overseas territory. Subsection (5) would enable the Commissioner to charge for assistance under subsection (4) if approved by the Secretary of State.

293 Subsection (6) defines the meaning of 'data protection functions', mutual assistance in the enforcement of legislation for the protection of personal data' and 'third party' for the purposes of this section.

Clause 119: Data-sharing code

294 This clause places an obligation on the Commissioner to publish and keep under review a data sharing code of practice. It preserves the effect of section 52A of the 1998 Act.

295 Subsections (1) and (2) require the code to contain guidance on data sharing and good practice. Good practice is defined as practice that appears to the Commissioner to be desirable including, but not limited to, compliance with the requirements of data protection legislation. The Commissioner can also make amendments to the code or prepare a replacement code should this be necessary.

296 Subsection (3) requires that in preparing the code the Commissioner must consult, as the Commissioner considers appropriate, with trade associations, data subjects and persons who represent the interests of data subjects.

Clause 120: Direct marketing code

297 This clause places the Commissioner under a duty to publish and keep under review a direct marketing code of practice. This preserves the effect of section 52AA of the Act 1998 Act.

298 Subsections (1) and (2) provide that the code will contain guidance about direct marketing and good practice. Good practice is defined as practice that appears to the Commissioner to be desirable including, but not limited to, compliance with the requirements of data protection legislation and the [Privacy and Electronic Communications \(EC Directive\) Regulations 2003 \[SI 2003/2426\]](#)⁸ ("PECR"). When deciding what constitutes good practice, the Commissioner must have regard to the interests of data subjects and others.

299 Subsection (3) requires that in preparing the code the Commissioner must consult, as he or she considers appropriate, with trade associations, data subjects and persons who represent the interests of data subject.

Clause 121: Approval of data-sharing and direct marketing codes

300 This clause sets out the process by which the Secretary of State must seek the approval of Parliament for codes prepared under clauses 119 and 120.

Clause 122: Publication and review of data-sharing and direct marketing codes

301 This clause sets out the process the Commissioner must follow when publishing a code prepared under clause 121 once it has been approved by Parliament. It also places a requirement on the Commissioner to keep the codes under review from the time they come into force, with a particular requirement placed on the Commissioner to amend the code in accordance with clauses 119(2) and 120(2) if he or she becomes aware that terms of such a code could result in a breach of an international obligation of the United Kingdom.

Clause 123: Effect of data-sharing and direct marketing codes

302 This clause sets out the legal effect of codes published under clause 121. It states that a code issued under clause 121(3) is admissible in evidence in legal proceedings; and that the Information Commissioner must take a relevant provision of the code into account when determining when determining a question arising in connection with the carrying out of the Commissioner's functions under the data protection legislation.

Clause 124: Other codes of practice

303 This clause provides the Secretary of State with the power to direct the Commissioner to produce other codes of practice for guidance as to good practice in the processing of personal data. The direction must describe the personal data or processing to which the code relates and may also describe the persons to which it relates. A definition of 'good practice in the

⁸ The Privacy and Electronic Communications (EC Directive) Regulations 2003 2003 No. 2426

processing of personal data’ is provided at subsection (4). Before preparing the code the Commissioner must consult any of those the Commissioner considers appropriate from the list at subsection (2).

Clause 125: Consensual audits

304 This clause replicates section 51(7) of the 1998 Act. Subsection (1) permits the Commissioner, with the consent of the data controller or processor, to carry out an assessment of whether the controller or processor is complying with good practice.

305 Subsection (2) requires the Commissioner to inform the controller or processor of the results of the assessment.

306 Subsection (3) defines the meaning of “good practice in the processing of personal data”.

Clause 126: Disclosure of information to the Commissioner

307 This clause makes clear that a person is not precluded by any other legislation from disclosing to the Commissioner information needed by the Commissioner in relation to the Commissioner’s functions under the legislation specified in subsection (2).

Clause 127: Confidentiality of information

308 Subsection (1) of this clause prevents persons who are currently or have previously been the Commissioner, a member of the Commissioner’s staff or an agent of the Commissioner from disclosing information obtained in connection with their investigations under the data protection legislation, the 2000 Act or the information regulations without lawful authority. It is an offence to knowingly or recklessly disclose information without lawful authority.

309 Subsection (2) provides the conditions for which information can be legally disclosed.

310 Subsection (3) defines the meaning of ‘information regulations’.

Clause 128: Guidance about privileged communications

311 This clause requires the Commissioner to produce and publish guidance on how she will (a) limit the use and disclosure of privileged communications she obtains or has access to during the course of carrying out her functions to ensure this goes no further than is necessary; and, (b) ensure that she does not have access to privileged communications which she is expressly prohibited from accessing under clause 138 (restrictions on information notices), clause 141 (restrictions on assessment notices), paragraph 12 of Schedule 15 (powers of entry and inspection) or under equivalent provisions in other enactments (as defined in clause 184).

312 Before publishing, replacing or making alterations to the guidance the Commissioner must consult the Secretary of State. She must also make arrangements for the guidance and any replacements or amendments to be laid before each House of Parliament.

313 Subsection (5) defines ‘privileged communications’ which clarifies the circumstances in which the guidance issued will apply (e.g. when the Commissioner is handling communications between a professional legal adviser and their clients made with a view to providing them with legal advice).

314 Subsection (6) confirms that the term ‘client’ in subsection (5) includes representatives of clients. It also confirms that the term ‘communication’ in subsection (5) includes copies and records of communications (e.g. telephone call recordings), and includes documentation enclosed or attached to communications under subsection (5).

Clause 129: Fees for services

315 The Commissioner can charge any person other than a person who is a data subject or a data protection officer to pay a fee for services that the Commissioner has services provided, either to the person or at their request, under the data protection legislation.

Clause 130: Manifestly unfounded or excessive requests by data subjects etc

316 This clause provides for the Commissioner to either charge a reasonable fee or refuse a request from a data subject of data protection officer which is unfounded or excessive, as required under Article 57 (4) of the GDPR.

317 Subsection (2) provides an example of a request that could be considered excessive.

318 Subsection (3) provides for the Commissioner to demonstrate that requests are excessive or unfounded, as required under Article 57 (4) of the GDPR.

Clause 131: Guidance about fees

319 This clause requires the Commissioner to prepare and publish guidance about the fees she proposes to charge in accordance with:

- clause 129 in relation to fees for services;
- clause 130 in relation to manifestly unfounded or excessive requests by data subjects or data protection officers; or
- Article 57(4) of the GDPR where requests are manifestly unfounded or excessive.

320 Before publishing the guidance, the Commissioner is required to consult the Secretary of State.

Clause 132: Charges payable to the Commissioner by controllers

321 This clause provides the Secretary of State with a power to make regulations requiring data controllers to pay a charge to the Commissioner. Those regulations may provide for different charges in different cases and for a discounted charge. In setting the charge the Secretary of State will take into account the desirability of offsetting the amount needed to fund the Commissioner's data protection and privacy and electronic communications regulatory functions. It also provides that the Secretary of State may make regulations requiring a controller to provide information to the Commissioner to help the Commissioner identify the correct charge.

322 This and the following clause reproduces the substance of the charging powers inserted into the 1998 Act by sections 108 to 110 of the Digital Economy Act 2017. These powers were originally legislated for ahead of this Bill to allow the new charges to be in place in time of the GDPR coming into force in May 2018.

Clause 133: Regulations under section 132: supplementary

323 Subsection (1) makes it a requirement for the Secretary of State to consult such representatives of persons likely to be affected by the regulations as the Secretary of State thinks appropriate and such other persons as the Secretary of State thinks appropriate, before making regulations under clause 132. Pursuant to clause 169 the Secretary of State must also consult the Commissioner.

324 The clause also provides a mechanism for review of the regulations and allows for a change to the charge in line with the RPI to be by negative procedure. All other regulations made under clause 132 are subject to the affirmative procedure.

Clause 134: Reporting to Parliament

- 325 Subsection (1) requires the Information Commissioner to produce a general report on the carrying out of the Commissioner's functions annually, lay it before Parliament and publish it. This clause largely replicates section 52(1) of the 1998 Act.
- 326 Subsection (2) explains that a report must include an annual report of its activities as stated in Article 59 of the GDPR.
- 327 Subsection (3) provides that the Commissioner can also lay other reports before the Houses of Parliament.

Clause 135: Publication by the Commissioner

- 328 Where the Commissioner has a duty to publish a document, this clause provides that it can be published in a way that the Commissioner considers appropriate.

Clause 136: Notices from the Commissioner

- 329 This clause outlines the procedures which may be followed by the Commissioner when required or authorised to issue a notice under this Bill. This provision largely replicates section 65 of the 1998 Act.

Part 6: Enforcement

Clause 137: Information notices

- 330 This clause makes provision about information notices. An information notice requires a controller or processor to provide the Commissioner with specified information within a certain time period.
- 331 Subsection (1) provides the Commissioner with a power to issue an information notice.
- 332 Subsection (2) provides that the information notice must explain why the information is needed.
- 333 Subsection (3) provides that the notice may include requirements about what information should be provided and how and when that information should be provided.
- 334 Subsection (4) requires an information notice to provide details about appeal rights
- 335 Subsection (5) provides that an information notice must not require the data controller or processor to comply with the measures in the notice before the end of the period in which an appeal could be brought.
- 336 Subsection (6) provides that if an appeal is brought, the controller or processor need not comply with the information notice until the appeal has been withdrawn or decided.
- 337 Subsection (7) provides that subsections (5) and (6) do not apply where the Commissioner considers there is an urgent need for the information in question. In these circumstances, however, the information notice must allow the controller/processor at least seven days to provide the information requested.
- 338 Subsection (8) provides that the Commissioner may cancel an information notice.

Clause 138: Information notices: restrictions

- 339 This clause seeks to replicate section 46 of the 1998 Act, which places certain restrictions on the Commissioner issuing information notices.

- 340 Subsection (1) provides that an information notice cannot be made in respect of personal data being processed for journalistic, academic, artistic or literary purposes, unless the Commissioner has made or is likely to make a written determination under clause 164 explaining why it would be justified.
- 341 Subsections (2) to (4) provide that an information notice cannot compel a person to provide the Commissioner with details of communications with legal advisers about their compliance with data protection legislation or in connection with any proceedings brought against them under the legislation.
- 342 Subsection (5) provides that an information notice cannot compel a person to provide information that would implicate them in any of the offences in this Bill or for other criminal offences listed in subsection (6). Where an information notice is served on the representative of a controller or processor who is based outside the UK, subsection (8) makes it clear that the representative is not required to provide information that would incriminate the controller or processor.
- 343 Subsection (7) provides that information provided in response to an information notice cannot be used as evidence in criminal proceedings brought under this Bill, unless the proceedings relate to the offence of failing to comply with an information notice under clause 137 regarding failing to comply with an information notice. The only other exceptions would be where the defendant gave evidence in court which was inconsistent with the evidence provided in his or her statement to the Commissioner, or where the defendant volunteered information from the statement during the course of proceedings.

Clause 139: Failure to comply with an information notice

- 344 Subsection (1) makes it an offence to fail to comply with an information notice and subsection (2) provides a defence where the person charged has exercised all due diligence to comply with the notice. As worded, this clause imposes a legal burden on the defendant to prove the defence on the balance of probabilities.
- 345 It is also an offence under subsection (3) for a person to intentionally or recklessly make a false statement in response to an information notice.
- 346 These provisions replicate the offences in section 47 of the 1998 Act insofar as they relate to failure to comply with an information notice.

Clause 140: Assessment notices

- 347 This clause replicates the provisions on assessment notices in section 41A of the 1998 Act.
- 348 Subsection (1) provides the Commissioner with a power to issue an assessment notice for the purpose of carrying an assessment of whether the controller or processor has complied or is complying with the data protection legislation.
- 349 Subsection (2) sets out what the Commissioner may require the controller or processor to do following receipt of an assessment notice. This may include, for example, permitting the Commissioner to enter specified premises, assist the Commissioner to view certain documents or to observe processing that takes place on the premises.
- 350 Subsection (4) requires the assessment notice to set out the times at which each requirement in the notice must be complied with.
- 351 Subsection (5) requires an assessment notice to provide information about rights of appeal under clause 154.

352 Subsection (6) prohibits an assessment notice from requiring the data controller or processor to do anything before the end of the period in which an appeal could be brought against the notice.

353 Subsection (7) provides that if an appeal is brought against the notice, the controller or processor need not comply with the notice until the appeal has been withdrawn or decided.

354 Subsection (8) provides that subsections (6) and (7) do not apply where the Information Commissioner considers there is an urgent need for the controller or processor to comply. In these circumstances, however, the assessment notice must allow the controller or processor a minimum of seven days to comply from the date the notice is given.

355 Subsection (9) permits the Commissioner to cancel an assessment notice by written notice to the controller or processor to whom it was given.

356 Subsections (10) and (11) are self-explanatory.

Clause 141: Assessment notices: restrictions

357 This clause seeks to replicate section 41B of the 1998 Act, which sets out certain limitations in respect of assessment notices.

358 Subsections (1) and (2) provide exemptions from complying with an assessment notice where this would result in disclosure of communications between a professional legal adviser and their client in respect of the client's obligations under the data protection legislation or in respect of proceedings brought against the client.

359 Subsection (3) explains the terms "client" and "communication" for the purposes of subsection (1) and (2).

360 Subsection (4) exempts a controller or processor from receiving an assessment notice if they are processing personal data for journalistic, academic, artistic or literary purposes.

361 Subsection (5) lists other bodies which are exempt from receiving an assessment notice.

Clause 142: Enforcement notices

362 Subsection (1) gives the Commissioner the power to issue an enforcement notice which requires a person to take steps or refrain from taking steps specified in the notice for failings or failures set out in subsections (2), (3), (4) and (5).

363 Subsection (2) sets out the circumstances in which a controller or processor can be issued with an enforcement notice for failure to comply with provisions in the GDPR and this Act listed in subsection (2)(a) to (e).

364 Subsection (3) enables the Commissioner to issue an enforcement notice when a monitoring body (of approved codes of conduct as defined in Article 41 of the GDPR) fails to comply with an obligation under Article 41.

365 Subsection (4) sets out the circumstances in which a certification provider can be issued with an enforcement notice. These are where the certification provider does not meet the requirements for accreditation; has failed or is failing to comply with an obligation under Article 42 or 43; or has failed or is failing comply with another provision of the GDPR – whether in their capacity as a certification provider or otherwise.

366 Subsection (5) enables the Commissioner to issue an enforcement notice against a controller for failure to comply with section 132 in respect of charges payable to the Commissioner.

367 Subsection (6) limits the requirements that the Commissioner may impose when issuing an enforcement notice under subsection (2), (3) or (5) to those which the Commissioner considers appropriate to remedy the failure committed.

368 Subsection (7) limits the requirements that the Commissioner may impose (which might include but doesn't have to include a requirement to remedy the failure) when issuing an enforcement notice under subsection (4) which she considers are appropriate with regard to the failure.

369 Subsection (8) provides the Secretary of State with a regulation making power to confer a power on the Commissioner to give an enforcement notice in respect of other failures not listed in this section. Subsection (9) requires the Secretary of State to consult such persons as they consider appropriate when making a regulation under subsection (8).

370 Subsection (10) sets out how regulations under this section can be used.

Clause 143: Enforcement notices: supplementary

371 This clause sets out supplementary provisions in respect of enforcement notices given under clause 142.

372 Subsections (1) and (2) are self-explanatory.

373 Subsection (3) explains that the enforcement notice issued by the Commissioner in relation to clause 142(2) and (1)(b) will also grant the Commissioner powers to suspend the data controller or processor from processing any data, or any specific type of data which is specified for a particular purpose, time or has a particular description.

374 Subsection (4) clarifies that the enforcement notice can establish the specific time and period within which the requirements set out in the enforcement notice must be complied with. Restrictions apply where during the appeal period, the requirements in the notice must not be issued, and need not be complied with until the conclusion or withdrawal of the appeal.

375 Subsection (5) is self-explanatory.

376 Subsections (6) and (7) sets out the exemptions to issuing specific requirements in an enforcement notice during the appeal period.

377 Subsection (8) states that subsections (6) and (7) do not apply if the enforcement notice explicitly states why the requirements must be complied with urgently. Furthermore, the Commissioner must not require the requirements to be complied with before the end of the 7 days from when the notice was issued.

378 Subsection (9) is self-explanatory.

Clause 144: Enforcement notices: rectification and erasure of personal data etc

379 Subsection (1) makes it clear that this clause applies where the enforcement notice relates to the controller or processor's failure to comply with the data protection principle relating to accuracy (as defined in subsection (8)). The clause may also apply where a controller or processor has failed to comply with data subjects' rights on rectification, erasure or restriction of processing under Articles 16 to 18 of the GDPR.

380 Subsection (2) states that if an enforcement notice requires a controller or processor to rectify or erase inaccurate personal data, it may also require the controller or processor to rectify or erase any expressions of opinion which are based on the inaccurate personal data. For example, if a bank holds inaccurate data about an individual's credit card repayments which leads them to conclude that person is not creditworthy, the Commissioner can require that data and any inaccurate conclusions flowing from it to be rectified or erased.

381 Subsection (3) sets out that if a data controller or processor has accurately recorded personal data provided by the data subject or a third party, which is later found to be inaccurate, the enforcement notice may require the controller or processor to ensure the data is rectified, or to supplement it with the data subject's view as to why it is inaccurate, or a statement of the true facts.

382 When considering what steps should be specified in an enforcement notice to rectify inaccurate data, subsection (4) provides the Commissioner must consider the purpose for which the data was obtained and further processed.

383 Subsections (5) to (7) provide that where an enforcement notice requires inaccurate data to be rectified, the notice may require the controller or processor to notify any third parties to whom the data may have been disclosed. The Commissioner must consider the number of people who would need to be notified when considering whether such notification would be practicable.

Clause 145: Enforcement notices: restrictions

384 This clause sets out certain restrictions which apply to the Commissioner when issuing enforcement notices to a data controller or processor. It reflects the provisions of Article 85 of the GDPR, which reconciles the protection of personal data with the right to freedom of expression for literary, artistic, journalistic or academic purposes. It replicates existing provisions under sections 46(1) and (2) of the 1998 Act.

385 Subsection (1) states that an enforcement notice cannot be served on a controller or processor if the processing was for artistic, journalistic, academic or literary purposes, unless the Commissioner has determined under clause 164 that the processing was not wholly for such purposes, or the court has granted permission for the enforcement notice to be served.

386 Subsection (2) provides that the court cannot grant leave for an enforcement notice to be served unless certain conditions are met.

Clause 146: Enforcement notices: cancellation and variation

387 This clause outlines the power invested to the Commissioner in Article 58(2) and 58(4) of the GDPR to cancel or amend an enforcement notice. It replicates the provisions enacted in section 41 of the 1998 Act.

388 Subsection (1) describes the way in which the Commissioner can communicate a decision to cancel or amend an enforcement notice to the controller or processor.

389 Subsection (2) states that a data controller or processor can apply to the Commissioner to have the enforcement notice varied or cancelled.

390 Subsection (3) sets out the grounds on which an application under subsection (2) can be made.

Clause 147: Powers of entry and inspection

391 This clause introduces Schedule 15 which makes provisions about the Commissioner's powers of entry and inspection.

Clause 148: Penalty notices

392 This clause seeks to replicate section 55A of the 1998 Act, which gives the Commissioner a power to serve a monetary penalty notice requiring the data controller to pay the Commissioner an amount determined by the Commissioner.

393 Subsection (1) sets out the circumstances in which the Commissioner can issue a written penalty notice requiring the controller or processor to pay the Commissioner a fine. These are

where the Commissioner is satisfied that a person has failed to comply with certain provisions of the GDPR or this Act or has failed to comply with an assessment notice or an enforcement notice.

394 Subsections (2) and (3) deal with the matters which the Commissioner must have regard to when considering deciding whether to give a penalty notice and determining the amount of the penalty.

395 Subsection (4) introduces Schedule 16 which makes further provision about penalty notices.

396 Subsection (5) provides the Secretary of State with a regulation making power that allows the Secretary of State to confer a power on the Commissioner to give a penalty notice for failures that are additional to those set out in subsection (1) and to make provision about the amount of penalty that may be imposed.

397 Subsection (6) requires the Secretary of State to consult such persons as the Secretary of State considers appropriate before making regulations under subsection (5).

398 Subsection (7) states that regulations under this section are subject to the affirmative resolution and may make provision about the giving of penalty notices and amend other provisions relating to such notices.

Clause 149: Penalty notices: restrictions

399 This clause sets out the restrictions placed on the Information Commissioner in relation to its ability to issue a penalty notice under clause 142(2) in relation to different types of processing.

400 Subsections (1) and (2) replicate section 46 of the 1998 Act. Subsection (1) provides the circumstances where the Commissioner cannot issue a penalty notice to a controller or processor for processing of personal data for the special purposes. Subsection (2) provides the condition for which a court must not provide grant of leave for a penalty notice to a controller or processor for processing of personal data for the special purposes.

401 Subsection (3) prohibits the Commissioner from issuing a penalty notice to the Crown Estate Commissioners or a person who is a controller under clause 188(3).

Clause 150: Maximum amount of penalty

402 This clause implements the requirements in Article 83 GDPR, for supervisory authorities to impose administrative fines on data controllers and processors who act in breach of the Bill. This clause also seeks to replicate parts of section 55A of the 1998 Act, which gives the Commissioner a power to serve a monetary penalty notice and impose a maximum penalty for breaches of the Act.

403 Subsection (1) specifies the maximum penalty that can be issued by the Commissioner's office on a penalty notice. Article 83 of the GDPR sets the maximum penalty that can be issued as 20 million EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

404 Subsection (2) provides that a maximum penalty amount imposed by a penalty notice is to be applied to breaches of Part 3 of the Bill.

405 Subsection (3) provides that a high maximum amount imposed by a penalty notice is to be applied to breaches of Part 4 of the Bill.

406 Subsection (4) sets a maximum penalty amount imposed by a penalty notice for failure to comply with an enforcement notice.

407 Subsection (5) sets what the higher maximum amount is. The higher maximum amount to be 20 million EUR or 4% of the undertaking's total annual worldwide turnover.

408 Subsection (6) sets the standard maximum amount to be 10 million EUR or 2% of the undertaking's total annual worldwide turnover

409 Subsection (7) outlines how to calculate the conversion of the maximum amount of a penalty in sterling.

Clause 151: Fixed penalties for non-compliance with charges regulations

410 This places an obligation on the Commissioner to publish a document specifying the penalty amounts for failure to comply with regulations under clause 132 (charges payable to the Commissioner by controllers). Different amounts may be specified for different types of failure.

411 Subsection (3) outlines the maximum fine that can be issued for non-compliance as 150% of the highest charge payable pursuant to regulations made under Clause 132.

412 Subsection (5) places an obligation on the Commissioner to consult the Secretary of State and such other person as the Secretary of State considers appropriate, before publishing the document.

Clause 152: Amount of penalties: supplementary

413 This clause provides the Secretary of State with the power to introduce regulations for the purposes of Article 83 of the GDPR and clause 151, using the affirmative resolution procedure.

Clause 153: Guidance about regulatory action

414 Subsection (1) requires the Commissioner to prepare and publish guidance about how she will exercise her functions in relation to assessment notices, enforcement notices and penalty notices. Subsection (2) enables the Commissioner to produce and publish guidance in respect of her other regulatory functions not listed in subsection (1).

415 Subsection (3) sets out the elements that must be included in the guidance on assessment notices and subsection (5) sets out the element that must be included in the guidance on penalty notices.

416 Subsection (6) allows the Commissioner to alter or replace the guidance. Subsection (7) requires the Commissioner to consult the Secretary of State and such other persons as the Secretary of State considers appropriate before publishing the guidance (including altered or replacement guidance).

Clause 154: Rights of appeal

417 This clause lists the five specific notices that can be appealed to the tribunal. When these notices have been categorised as urgent an appeal can be made against the urgent element, even if rest of the notice is not being appealed against.

418 The value of the penalty can be appealed, even where the notice is not being appealed.

419 Where the Commissioner has made a ruling on the use of personal data in relation to "special purposes" (journalism, academic, artistic or literary purposes) the controller or processor may appeal to the tribunal against the decision.

Clause 155: Determination of appeals

420 When an appeal has been made to the tribunal on the grounds of clause 154(1) or (4) the tribunal can review any determination of fact on which the notice or decision against which

the appeal is brought was based. When (a) the notice is not within the law or (b) when the Commissioner should have exercised her discretion differently, the tribunal should (a) uphold the appeal, (b) issue another notice or (c) alter the decision made by the Commissioner.

421 When an appeal has been made on the grounds of clause 154(3) or (5) the tribunal has the authority to cancel the notice or the Commissioner's determination.

Clause 156: Complaints by data subjects

422 This clause sets out a data subject's right to make a complaint to the Commissioner about an infringement of the data protection legislation in relation to his or her personal data. This right reflects Articles 57 and 77 of the GDPR and Article 41 of the LED.

423 Subsection (1) signposts the right of the data subject to complain under Articles 57 and 77 of the GDPR.

424 Subsection (2) gives the data subject the right to complain to the Commissioner if there has been an infringement of Part 3 or Part 4 of the Act relating to their personal data.

425 Subsection (3) requires the Commissioner to facilitate the making of complaints, including by providing a complaint form in either electronic or paper format.

426 Subsection (4) explains the steps which the Commissioner must take when dealing with a complaint. These include taking appropriate steps to respond to the complaint, informing the data subject of the outcome of the complaint, and informing the data subject of their right to apply for an order from the tribunal against the Commissioner. If asked by the complainant, the Commissioner is also required to give the data subject further information about how to proceed with the complaint.

427 Subsection (5) explains that the requirement for the Commissioner to take "appropriate steps" to respond to a complaint includes investigating the complaint, to the extent appropriate, as well as informing the complainant about progress with the complaint and whether further investigation or coordination with another authority is necessary.

428 Subsection (6) provides that where the Commissioner receives a complaint which relates to an infringement of another Member State's legislation implementing the LED, the Commissioner must pass on that complaint to the supervisory authority of the relevant Member State. The Commissioner must inform the complainant that this has been done, and if asked to do so must provide further information about how to proceed with the complaint.

429 Subsection (7) defines the other authorities with whom the Commissioner may be required to co-ordinate in dealing with the complaint.

430 The provisions in this clause are broadly equivalent to section 42 of the 1998 Act, while taking account of the expanded rights of data subjects under the GDPR, the LED and this Bill.

Clause 157: Orders to progress complaints

431 This clause enables a data subject to apply for an order from the tribunal if the Commissioner does not take certain actions in relation to a complaint made by the data subject. This is a new provision and has no equivalent in the 1998 Act. It reflects the rights set out in Article 78(2) of the GDPR and Article 53(2) of the LED.

432 Subsection (1) sets out the circumstances in which an application can be made to the tribunal. These are if the Commissioner fails to take appropriate steps to respond to a complaint, or fails to update the data subject on progress with the complaint or the outcome of the complaint within three months after the submission of the complaint, or any subsequent three month period in which the Commissioner is still considering the complaint.

433 Subsection (2) explains that following an application by the data subject the tribunal can order the Commissioner to take appropriate steps to investigate the complaint, or to notify the data subject of the progress or outcome of the complaint, within a specified period set by the tribunal.

434 Subsection (3) provides that the tribunal's order may require the Commissioner to take certain specified steps, or to conclude the investigation or take a specified step within a specified period.

435 Subsection (4) clarifies that for the purposes of subsections (1)(a) and (2)(a), "appropriate steps" has the same meaning as that set out in clause 156(5).

Clause 158: Compliance orders

436 This clause gives a data subject the right to apply for a court order against a controller or processor if their rights under the data protection legislation (other than Part 4) have been infringed – for example, their rights to access, portability, rectification and erasure. This gives effect to the rights in Article 79 of the GDPR and Article 54 of the LED and is broadly equivalent to the rights to apply for court orders which are set out under sections 7, 10, 11, 12 and 14 of the 1998 Act, but also extends to the new rights given by the GDPR and the LED. (This clause does not apply to infringements of Part 4, as there are separate provisions in Part 4 enabling data subjects to apply for court orders).

437 Subsection (1) sets out the right to apply for a court order if the data subject's rights have been infringed.

438 Subsection (2) sets out the powers exercisable by the court. The court can make an order against the controller in relation to the processing, or a processor acting on that controller's behalf. The court order can instruct the controller or processor to take certain steps as specified in the court order, or to refrain from taking certain steps.

439 Subsection (3) explains that the court order may specify when the steps in the order must be taken, or the period during which they must be taken.

440 Subsection (4) confirms that a data subject can apply for a court order under this clause in relation to an infringement of their rights under the GDPR, in accordance with Article 79(1) of the GDPR, but not in relation to an infringement of their rights under Part 4.

441 Subsection (5) provides that where there are joint controllers under Part 3 or Part 4 whose responsibilities have been determined in accordance with the relevant provisions in Part 3 or Part 4, the court can only make an order against the controller which is responsible for complying with the provision of the data protection legislation which has been breached.

Clause 159: Compensation for contravention of the GDPR

442 This clause makes provision in relation to the right to compensation under Article 82 of the GDPR. Article 82 gives a person the right to receive compensation from a controller or processor if they have suffered damage as a result of an infringement of the GDPR. The right to receive compensation set out in Article 82 is broadly equivalent to section 13 of the 1998 Act, with the exception that the type of damage which can be claimed is broader than that provided for in the 1998 Act.

443 Subsection (2) and (3) provide that where proceedings for compensation are brought by a representative body on behalf of a data subject under Article 82 of the GDPR and the court orders that compensation should be paid, the court can provide that the compensation should be paid on behalf of the data subject to the representative body, or such other person as the court sees fit.

Clause 160: Compensation for contravention of other data protection legislation

- 444 This clause provides in subsection (1) that a person has the right to compensation from a controller or processor if they suffer damage because of a contravention of the data protection legislation. This clause does not apply to compensation for a contravention of the GDPR, which is dealt with separately in clause 159. As with clause 159 this right to receive compensation is broadly equivalent to section 13 of the 1998 Act, with the exception that the type of damage which can be claimed is broader than that provided for in the 1998 Act.
- 445 Subsection (2) sets out the situations in which a controller or processor is liable for damage. A controller is liable for the damage caused by processing if they are involved in the processing. A processor is liable for damage caused by processing which they are involved in only if they have acted in breach or outside of the controller's lawful instructions, or alternatively if they have not complied with an obligation under the data protection legislation which is specifically directed at processors.
- 446 Subsection (3) explains that a controller or processor is not liable for the damage if they can prove that they are not responsible in any way for the event giving rise to the damage.
- 447 Subsection (4) provides that where there are joint controllers under Part 3 or Part 4 whose responsibilities have been determined in accordance with the relevant provisions in Part 3 or Part 4, a controller is only liable for damage if that controller is responsible for complying with the provision of the data protection legislation which has been breached.
- 448 Subsection (5) sets out the same definition of damage which applies to clause 159, which includes distress.

Clause 161: Unlawful obtaining etc of personal data

- 449 This clause criminalises the deliberate or reckless obtaining, disclosing and retention of personal data without the consent of the data controller.
- 450 Subsection (1) sets out the elements of the offence. These reflect the elements of the previous offence in section 55 of the 1998 Act, except for the addition of unlawful 'retention' of data. This has been added to deal with situations where a person obtains data lawfully but then intentionally or recklessly retains it without the consent of the controller.
- 451 Subsections (2) and (3) provide defences where, for example, the data was obtained for the purposes of preventing or detecting crime, to fulfil a legal obligation, for reasons of public interest or for acting in the reasonable belief that they had a legal right or would have had the consent of the data controller. As worded, the clause places a legal burden on the defendant to prove the relevant defences on the balance of probabilities.
- 452 Subsections (4) to (6) make it an offence to sell or offer to sell personal data that was obtained, disclosed or retained unlawfully.

Clause 162: Re-identification of de-identified personal data

- 453 This clause creates a new offence of knowingly or recklessly re-identifying information that has been de-identified without the consent of the controller who de-identified the data. This responds to concerns about the security of de-identified data held in online files. For example, recommendations in the Review of Data Security, Consent and Opt-Outs by the National Data Guardian for Health and Care called for the Government to introduce stronger sanctions to protect de-identified patient data.
- 454 Subsection (1) sets out the elements of the offence.

455 Subsection (2) defines the meaning of “de-identification” and “re-identification” for the purposes of the offence and reflects the definition of pseudonymisation in Article 4(5) of the GDPR.

456 Subsections (3) provides the defendant with a defence if he or she can prove that re-identification was necessary for the purposes of preventing crime, for complying with a legal obligation or was justified as being in the public interest.

457 Subsection (4) provides further defences where the defendant can prove that he or she had reasonable belief that he or she had the consent of the data subjects to whom the information relates; or had the consent of the data controller responsible for de-identifying the information, or would have had such consent if that controller had known about the circumstances of the processing.

458 Subsection (5) creates a related offence of knowingly or recklessly processing personal data that has been unlawfully re-identified.

459 Subsection (6) provides a defence where the person charged with an offence under subsection (5) can prove that processing of the re-identified information was necessary for the purposes of preventing crime, for complying with a legal obligation or was justified as being in the public interest.

460 Subsection (7) provides further defences where the person can prove that he or she acted in the reasonable belief that the processing was lawful or that he or she had the consent of the controller who had de-identified the information or would have had such consent if the controller had known about the processing.

461 As worded, the clause places a legal burden on the defendant to prove the relevant defences on the balance of probabilities.

Clause 163: Alteration etc of personal data to prevent disclosure

462 This clause criminalises the alteration of personal data to prevent disclosure following the exercise of a subject access right. The relevant subject access rights are set out in subsection (2).

463 This offence is modelled on the offence in section 77 of the 2000 Act which is committed when somebody alters records to frustrate a request for information made under that Act. Unlike the offence in section 77 of that Act which applies only to public authorities, subsection (4) makes it clear that this offence can be committed by any data controller.

464 Subsection (5) provides for defences for this offences where the defendant can prove that the alteration of the data was justified. As worded, the clause places a legal burden on the defendant to prove the relevant defences on the balance of probabilities.

Clause 164: The special purposes

465 This clause defines special purposes as one or more of: the purposes of journalism, academic purposes, artistic purposes and literary purposes. It also defines special purposes proceedings as legal proceedings against a controller or processor relating to the processing of personal data processed for special purposes. The inclusion of academic purposes extends the existing special purposes definition under section 3 of the 1998 Act to include academic purposes in line with Article 85 of the GDPR.

466 Under this clause, the Commissioner may make a written determination in relation to the processing of personal data for the defined special purposes where that data: is not being processed solely for the special purposes; is not being processed with a view to the publication of new material in relation to the special purposes; or the processing in question would not be incompatible with the special purposes. The clause requires the Commissioner

to provide written notice of any determination made to the controller and processor concerned. The clause also sets out the conditions that must be met before the Commissioner's determination can take effect and requires the Commissioner to provide information about the relevant rights of appeal.

Clause 165: Provision of assistance in special purposes proceedings

- 467 This clause allows for individuals who are a party, or a prospective party, to special purposes related proceedings (as defined in clause 164) to apply to the Commissioner for assistance in those proceedings. It requires the Commissioner to decide whether, and to what extent, to grant assistance, but stipulates that the Commissioner must only approve the application if the case, in the Commissioner's opinion, involves a matter of substantial public importance. The clause also requires the Commissioner to notify the applicant as soon as reasonably practicable of a decision either way in respect of granting assistance.
- 468 If the Commissioner decides that the matter is not of substantial public importance, the clause requires reasons to be given.
- 469 If the Commissioner decides that the matter is of substantial public importance, and therefore to grant assistance, the clause requires the Commissioner to ensure that the person against whom the proceedings are is notified of the decision, as well as the applicant. The Commissioner is also required to give the applicant details of the assistance to be provided. The clause permits the Commissioner to either pay the costs in connection with the proceedings or indemnify the applicant for liability to pay costs, expenses or damages in connection with the proceedings.
- 470 The clause also makes provision for the Commissioner to recover expenses incurred as a result of granting assistance on a priority basis should the applicant be paid sums of money as a result of the proceedings.

Clause 166: Staying special purposes proceedings

- 471 This clause requires the court or tribunal to stay the special purposes proceedings if it appears to the court or tribunal, or if the controller or processor claim, that personal data to which the proceedings relate: is being processed only for special purposes; is being processed with a view to publication by persons of journalistic, literary, or artistic material; and has not been published before by the controller (with publication of the same material 24 hours prior to the relevant time to be ignored). The clause also sets out the conditions under which the stay can be lifted.

Clause 167: Jurisdiction

- 472 This clause sets out the courts by whom the jurisdiction conferred by specific provisions in the Bill is exercisable. In England and Wales and Northern Ireland the jurisdiction is exercisable by the county court or the High Court, and in Scotland by the sheriff or the Court of Session. This mirrors the jurisdiction provisions which applied to the exercise of similar rights under the 1998 Act.
- 473 Subsection (2) sets out the relevant provisions of the Bill and the GDPR to which the jurisdiction provision applies.
- 474 Subsection (3) explains that where Part 4 applies to the processing, the jurisdiction is exercisable only by the High Court (for cases in England and Wales and Northern Ireland), or the Court of Session (for cases in Scotland).

Clause 168: Interpretation of Part 6

- 475 This clause provides an interpretation of the terms used in Part 6 of the Act.

Part 7: Supplementary and final provision

476 In this part references to the GDPR are to the GDPR read with Chapter 2 of Part 2 and include the applied GDPR read with Chapter 3 of Part 2; references to processing and personal data are to processing and personal data to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies.

Clause 169: Regulations and consultation

477 This clause sets out the courts by whom the jurisdiction conferred by specific provisions in the Bill is exercisable. In England and Wales and Northern Ireland the jurisdiction is exercisable by the county court or the High Court, and in Scotland by the sheriff or the Court of Session. This mirrors the jurisdiction provisions which applied to the exercise of similar rights under the 1998 Act.

478 Subsection (2) sets out the relevant provisions of the Bill and the GDPR to which the jurisdiction provision applies.

479 Subsection (3) explains that where Part 4 applies to the processing, the jurisdiction is exercisable only by the High Court (for cases in England and Wales and Northern Ireland), or the Court of Session (for cases in Scotland).

Clause 170: Power to reflect changes to the Data Protection Convention

480 This clause provides the Secretary of State with a power (subject to the affirmative procedure) to make provisions necessary or appropriate in connection with amendment or replacement of the Data Protection Convention 108 which has or is expected to have effect in the United Kingdom.

Clause 171: Prohibition of requirement to produce relevant records

481 This clause makes it an offence for an employer to require employees or contractors, or for a person to require another person who provides goods, facilities or services, to provide certain records obtained via subject access requests as a condition of their employment or contract. It is also an offence for a provider of goods, facilities or services to the public to request such records from another as a condition for providing a service. Such conduct may give the employer or provider access to records which they would not otherwise have been entitled. There are established legal routes for employers and public service providers to carry out background checks, which do not rely on them obtaining information via subject access requests.

482 Subsections (1) and (2) set out the elements of the offence and subsection (3) provides for certain defences; i.e. to fulfil a legal obligation or if in the public interest. As worded, the clause places a legal burden on the defendant to prove the relevant defence on the balance of probabilities.

483 Subsection (5) defines what it means to place a “requirement” on somebody to provide relevant records. It includes any action that the person knows will make the other person feel obliged to comply with the request, or being reckless as to whether the person may feel that they are obliged to comply.

484 Subsection (6) defines the meaning of ‘employment’ and ‘relevant record’ for the purposes of the offence. More detail on relevant records is set out in Schedule 17.

485 This clause is similar to section 56 of the 1998 Act, but the list of relevant records in Schedule 17 is wider because it now includes medical records.

Clause 172: Avoidance of certain contractual terms relating to health records

486 This clause replaces section 57 of the 1998 Act. Subsections (1) to (3) make it clear that a term or condition of a contract is void if it requires an individual to supply all or part of a health record which has been obtained through the exercise of subject access rights.

487 Subsection (4) sets out the meanings of the terms “data subject access rights” as it applies in this clause.

Clause 173: Representation of data subjects

488 This clause concerns the ability of representative bodies to exercise certain rights on behalf of data subjects, provided they are authorized to do so by the data subjects. The relevant rights are the right to complain to the Commissioner, the right to bring judicial review proceedings against the Commissioner and to apply for a tribunal order against the Commissioner under clause 158, the right to apply for a court order against a controller or processor, and (in relation to the GDPR only) the right to receive compensation from a controller or processor. This clause reflects the rights in 80(1) of the GDPR and Article 55 of the LED.

489 Subsection (1) signposts to the right to authorise a representative body set out in Article 80(1) of the GDPR and allows a data subject to authorise a representative body to exercise his or her right to compensation under the GDPR.

490 Subsection (2) sets out, in relation to the data protection legislation other than the GDPR and Part 4, the right for a data subject to authorise a representative body to exercise his or her rights. It lists the rights a representative organisation can exercise on behalf of the data subject.

491 Subsections (3) and (4) sets out the requirements that a representative body must meet in order to exercise a data subject’s rights on their behalf. The representative body must be a not-for-profit organisation with objectives in the public interest, and must be active in protecting the rights and freedoms of data subjects in relation to their personal data.

492 Subsection (5) explains that references to a “representative body” in this Bill are to a body or organisation which is authorised to exercise a right on behalf of a data subject.

493 This is a new provision with no direct equivalent in the 1998 Act.

Clause 174: Data subject’s rights and other prohibitions and restrictions

494 This Bill gives the data subject rights and data controller obligations special status. This clause provides that any other enactment or rule of law that seeks to prohibit or restrict the giving of information or withholding of information specified shall not apply. The only restrictions that can exist are therefore the exemptions contained in this Bill.

Clause 175: Penalties for offences

495 This clause sets out the penalties for the offences in this Bill.

496 Subsection 1 sets out the penalties for the summary only offences in clauses 117 (inspection of personal data in accordance with international obligations), 163 (alteration of personal data to prevent disclosure) and paragraph 15 of Schedule 15 (obstructing the execution of a warrant). The maximum penalty on summary conviction is an unlimited fine in England and Wales or a Level 5 fine in Scotland and Northern Ireland.

497 Subsection (2) sets out the maximum penalties for offences that can be tried summarily or on indictment. These include offences in clauses 127 (confidentiality of information), 139 (failure to comply with an information notice), 161 (unlawful obtaining of personal data), 162 (re-identification of de-identified personal data) and 171 (prohibition of requirement to produce relevant records). In England and Wales, the maximum penalty when tried summarily or on

indictment is an unlimited fine. In Scotland and Northern Ireland, the maximum penalty on summary conviction is a fine not exceeding the statutory maximum or an unlimited fine when tried on indictment.

498 Subsection (4) provides a power for the court to order the forfeiture and destruction of material obtained under offences in clauses 161 and 171. Subsection (5) provides any individual (other than the offender) with an interest in the data the right to demonstrate to the court why they should not forfeit or destroy such material.

Clause 176: Prosecution

499 This clause makes it clear which enforcement agencies are responsible for prosecuting offences under this Bill. Subsection (1) provides that in England and Wales, prosecutions can be brought by the Commissioner or by, or with the consent of, the Director of Public Prosecutions. Subsection (2) provides that prosecutions in Northern Ireland can be brought by the Commissioner or by, or with the consent of, the Director of Public Prosecutions for Northern Ireland. In Scotland, the Procurator Fiscal handles all prosecutions in the public interest. There is therefore no need for the kind of provision made in this clause for Scotland as for other parts of the UK.

500 Subsections (3) to (7) set out periods allowed for prosecutions for an offence under clause 163 of this Bill (alteration etc. of personal data to prevent disclosure).

Clause 177: Liability of directors etc

501 This clause allows proceedings to be brought against a director, or person in or acting in a similar position, as well as the body corporate where it is proved that breaches of the Act have occurred with the consent, connivance, or negligence of that person.

502 The provision in this clause will have the same effect as that of section 61 of the 1998 Act.

Clause 178: Recordable offences

503 This clause allows for convictions for the offences in this Bill to be recorded on the Police National Computer and for the National Police Records (Recordable Offences) Regulations 2000 [SI 2000/1139] to have effect, as if amended by this Bill Offenders who are arrested for a recordable offence may have their fingerprints and DNA samples taken.

504 This clause extends to England and Wales only. Separate arrangements exist in Northern Ireland and Scotland for recording criminal offences.

Clause 179: Guidance about PACE codes of practice

505 Subsection (1) requires the Commissioner to publish guidance about how the Commissioner intends to perform the duty under section 67(9) of the Police and Criminal Evidence Act 1984 (duty to have regard to codes of practice under that Act when investigating offences and charging offenders).

506 Subsection (2) allows the Commissioner to alter or replace the guidance and requires the Commissioner to publish any altered or replacement guidance.

507 Subsection (3) provides that the Commissioner must consult the Secretary of State before publishing or amending guidance under this section.

508 Subsection (4) provides that any guidance produced, or amendments, must be laid before each House of Parliament.

Clause 180: Disclosure of information to the Tribunal

509 This clause permits a person to provide a tribunal with any information which is necessary for it to discharge its functions under the data protection legislation, the 2000 Act and the information regulations even if disclosing such information is prohibited under common law or other enactments.

Clause 181: Proceedings in the First-tier Tribunal: contempt

510 This clause allows the First-tier Tribunal to certify an offence to the Upper Tribunal if a person does something (or fails to do something) in relation to tribunal proceedings which would constitute contempt of court if the proceedings were before a court.

511 Subsection (1) explains the circumstances in which the offence can be committed, in relation to appeal proceedings or an application for an order from the First-tier Tribunal.

512 Subsections (2) and (3) provides that the First-tier Tribunal may certify an offence under subsection (1) to the Upper Tribunal, which in turn may inquire into the matter and deal with the person charged with offence in the same way in which it could deal with the person if the offence if it had been committed in relation to the Upper Tribunal.

513 Subsection (4) requires the Upper Tribunal to hear any witnesses and any statement offered in defence before exercising the power to deal with the person charged with the offence.

514 This provision replicates paragraph 8 of Schedule 6 to the 1998 Act with the exception that instead of certifying the contempt of court offence to the High Court, under this clause the First-tier Tribunal will now certify the offence to the Upper Tribunal.

Clause 182: Tribunal Procedure Rules

515 This clause sets out, in subsection (1), the power to make Tribunal Procedure Rules to regulate the way in which the rights of appeal before the tribunal and the right to apply for an order from the tribunal (which are conferred under the Bill) are exercised. It also allows tribunal Procedure Rules to be made about the exercise of a data subject's right to authorise a representative body to apply for an order on his or her behalf, under Article 80 of the GDPR and clause 173 of this Bill.

516 Subsection (2) also allows Tribunal Procedure Rules to be made about securing the production of material used for the processing of personal data, and inspecting, examining, operating and testing equipment or material used for the processing of personal data.

517 The provisions of this clause are equivalent to paragraph 7 of Schedule 6 to the 1998 Act. Any Tribunal Procedure Rules made under this clause will be made in accordance with the procedure set out in the Tribunals, Courts and Enforcement Act 2007.

Clause 183: Meaning of “health professional” and “social work professional”

518 Article 9(2)(h) and (i) of the GDPR permit processing of personal data which is necessary for health or social care purposes or for processing for public health purposes in the public interest where provided for in Union or Member State law. Clause 9(2) and paragraphs 2 and 3 of Schedule 1 permit processing for these purposes. Processing under Article 9(2)(h) is only permitted if the data is processed in accordance with Article 9(3) of the GDPR (professional secrecy obligations etc.). Clause 10(1) provides that those who are permitted to process personal data under Article 9(2)(h), by virtue of Article 9(3), include anyone processing data who is, or is under the supervision of, a “health professional” or a “social work professional”. Under paragraph 3 of Schedule 1 to this Bill, processing in the public interest for public health purposes may only be carried out in certain specified circumstances, including by, or under the supervision of a “health professional”.

519 Paragraph 8 of Schedule 3 to the 1998 Act similarly permitted the processing of sensitive personal data for medical purposes as long as it was undertaken by a health professional or a person under a duty of confidentiality. Section 69 of the 1998 Act, defined "a health professional" by way of a list.

520 In line with the approach taken to define health professional in section 69 of the 1998 Act, this clause provides a definition of "health professional", and also now includes a definition of "social work professional".

521 Subsection (1) provides a definition of "health professional" which includes: registered doctors; nurses; dentists; midwives; opticians; pharmacists and child psychotherapists.

522 Subsection (2) provides a definition of "social work professional", which includes registered social workers in England, Wales, Scotland and Northern Ireland.

523 Subsection (3) clarifies the definition of "a registered medical practitioner".

524 Subsection (4) defines a "health service body"; the definition varies in England, Wales, Scotland and Northern Ireland.

Clause 184: Other definitions

525 This clause is self-explanatory in defining terminology used in this Bill.

526 "Biometric data" includes DNA profiles held on the police National DNA Database, fingerprints (dactyloscopic data) stored on the National Fingerprint Database and facial images held on the Police National Database.

Clause 185: Index of defined expressions

527 This clause defines or explains terms and is self-explanatory.

Clause 186: Territorial application of this Act

528 This clause provides details of the territorial application of the Bill. Its application to data controllers and data processors depends on the place of establishment and the context of the activities of the establishment in which the personal data is processed.

529 Subsections (1) and (2) concern the application of the Bill as a whole to data controllers and data processors respectively.

530 Subsections (3) and (4) make limited extra-territorial application for Chapter 2 of Part 2 of the Bill only for data controllers and data processors respectively, in accordance with Article 3(2) of the GDPR.

531 The clause also defines a "person established in the United Kingdom". This includes an individual who is ordinarily resident in the UK, a body incorporated under UK law, a partnership or other unincorporated association formed under UK law, a person who maintains in the UK an office, branch or agency through which they carry out an activities or other stable arrangements.

Clause 187: Children in Scotland

532 This clause should be read in conjunction with clause 8. Clause 8 sets the age at which a child a child can give consent to the processing of their personal data by information society services. This clause then provides for when a child in Scotland, if old enough to give consent, should be considered as having the capacity to exercise their rights as under this Act and the GDPR.

533 In Scotland, persons under the age of 16 are taken to have the capacity to exercise rights under the 1998 Act if they have a general understanding of what it means to exercise that right and a person aged 12 or over is presumed to have that capacity. Subsections (2) and (3) of this clause provide that a child or young person under 16 can exercise their rights or give consent under the data protection legislation if the child or young person understands what it means to exercise that right or give such consent. A person aged 12 or over is to be presumed to be of sufficient age and maturity to have such understanding unless it is proved otherwise.

534 This clause is to be read in conjunction with Article 8 of the GDPR. Article 8, read with clause 8 of the Bill, provides that, in relation to the offer of information society services directly to a child, where the child has themselves given consent to the processing of their personal data, processing shall be lawful where the child is at least 13 years old. Where the child is below the age of 13 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

535 The age threshold in Article 8 GDPR means that no question can arise as to whether a child aged under 13 years old can lawfully give consent to the processing of their data in respect of information society services.

Clause 188: Application to Crown

536 The GDPR does not contain any provision to exempt the Crown from its requirements. Likewise, section 63 of the 1998 Act binds the Crown. This clause makes similar provision.

Clause 189: Application to Parliament

537 The GDPR does not contain any provision to exempt Parliament from its requirements. Likewise, section 63A of the 1998 Act applies that Act to the processing of personal data by or on behalf of either House of Parliament. This clause makes similar provision, save for Parts 3 and 4 of the Bill.

Clause 190: Minor and consequential amendments

538 This clause provides for minor and consequential amendments to other legislation, which follow as a consequence of the GDPR and this Bill. The minor and consequential amendments are contained in Schedule 18 and include the repeal of the 1998 Act. The clause confers on the Secretary of State a regulation-making power to make further consequential amendments, which arise from this Bill. Such regulations may also make transitional, transitory or saving provisions and amend, repeal or revoke an enactment. Any regulations that amend or repeal primary legislation are subject to the affirmative procedure. Any other regulations in this section are subject to the negative procedure.

Clause 191: Commencement

539 This clause provides the Secretary of State with a power to make regulations bringing the Bill into force. Certain provisions listed in subsection (2) come into force on the date of Royal Assent.

Clause 192: Transitional provision

540 This clause contains a power for the Secretary of State to make regulations making further necessary transitional, transitory or saving provision in connection with the coming into force of any provision of the Bill.

Clause 193: Extent

541 Detailed analysis of the extent of the Bill can be found at Annex D. Otherwise this clause is self-explanatory.

Clause 194: Short title

542 This clause is self-explanatory.

Schedule 1: Special categories of personal data and criminal convictions etc data

543 This Schedule specifies the conditions and associated safeguards that must be met in order for special categories of data to be processed pursuant to clause 9.

544 Part 1 specifies the conditions that must be met in order for special categories of data and personal data relating to criminal convictions and offences or related security measures (“criminal convictions etc.”) to be processed for employment, health, archiving and research purposes. It also provides specific safeguards for processing of special categories of data for health purposes.

545 Part 2 specifies the conditions that must be met in order for special categories of data and personal data to be processed for reasons of substantial public interest. Personal data relating to criminal convictions etc. may also be processed under relevant conditions in this Part.

546 Part 3 specifies the additional conditions that must be met in order for personal data relating to criminal convictions etc. to be processed otherwise than under the control of official authority.

547 Part 4 specifies additional safeguards that must be applied where processing is undertaken in reliance on paragraph 1 of Schedule 1, Part 2 of Schedule 1, and paragraphs 27 and 28 of Schedule 1. These safeguards apply in addition to any express safeguards provided for in Parts 1 to 3.

Part 1 - Conditions relating to employment, health, research etc

548 Paragraph 1 relates to Article 9(2)(b) of the GDPR and allows the processing of special categories of data in the field of employment, social security and social protection law where necessary for the purposes of performing or exercising obligations or rights of the controller or the data subject. This condition is only met if the controller has an appropriate policy document in place (as defined in Part 4).

549 Paragraph 2(1) relates to Article 9(2)(h) of the GDPR, and enables processing of special categories of data for health or social care purposes. These purposes are defined as “health or social care purposes” in paragraph 2(2) and include all purposes listed in Article 9(2)(h). Paragraph 2(3) signposts the conditions and safeguards in Article 9(3) of the GDPR that apply to processing under Article 9(2)(h), and clause 10(1), which defines circumstances that are included in the Article 9(3) requirement.

550 Paragraph 3 relates to Article 9(2)(i) of the GDPR, and enables processing of special categories of data for the purposes of public interest in the area of public health. Processing under this condition must be carried out by, or under the supervision of, a health professional, or by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

551 Paragraph 4 relates to Article 9(2)(j) of the GDPR, and allows processing that is necessary for archiving purposes, scientific or historical research purposes or statistical purposes if the processing is carried out in accordance with Article 89(1) of the GDPR (as supplemented by clause 18) and is in the public interest.

Part 2 - Substantial public interest conditions.

- 552 This Part relates to Article 9(2)(g) of the GDPR and sets out the conditions for processing of special categories of data which are necessary for reasons of substantial public interest. The majority of these processing conditions existed in or under Schedule 3 to the 1998 Act and the effect of those conditions is retained, with adjustments, in this Bill.
- 553 Paragraph 5 makes it a condition of processing under this Part for the data controller to have appropriate safeguards in place as set out in Part 4.
- 554 Paragraph 6 permits processing of special categories of data that is in the substantial public interest and is necessary for the administration of justice; the exercise of a function of either House of Parliament; the exercise of a function conferred on a person by an enactment or the exercise of a function of the Crown, a Minister of the Crown or a Government department.
- 555 Paragraph 7 permits processing of personal data revealing health or ethnic origin, personal data revealing religious or philosophical beliefs, data concerning health and personal data concerning an individual's sexual orientation for the monitoring of equality between persons with different racial or ethnic origins, different religious or philosophical beliefs, differing physical or mental health conditions or between persons of different sexual orientation. Processing does not meet this condition if it is carried out for the purposes of measures or decisions with respect to the particular data subject unless the data subject has consented. Processing also does not meet this condition if it is likely to cause substantial damage or distress to the data subject. An individual can give notice in writing to the controller requiring the controller to cease processing his or her data, and the processor must cease processing within a reasonable period.
- 556 Paragraph 8 permits processing of special categories of data for the purposes of the prevention or detection of any unlawful act where seeking the consent of the data subject to the processing would prejudice those purposes and it is necessary for reasons of substantial public interest.
- 557 Paragraph 9 permits processing of special categories of data which is necessary for the purposes of discharging certain protective functions which are designed to protect members of the public from certain conduct which may not constitute an unlawful act, such as dishonesty, incompetence or mismanagement. Additional requirements are that seeking the consent of the data subject would prejudice those purposes and the processing is necessary for reasons of substantial public interest.
- 558 Paragraph 10 permits processing of special categories of data which is necessary for the disclosure of data for journalism, academic, artistic or literary purposes where the subject matter of the disclosure relates to the matters mentioned in sub-paragraph (2) (unlawful acts; dishonesty, malpractice or other seriously improper conduct; unfitness or incompetence, mismanagement or a failure in services). The disclosure must be carried out with a view to the publication of the personal data by any person and it must be necessary for reasons of substantial public interest. In addition, the controller must reasonably believe that publication of the personal data would be in the public interest.
- 559 Paragraph 11 permits the processing of special categories of data where the disclosure is necessary for preventing fraud, or a particular type of fraud, and is by a member of an anti-fraud organisation (as defined in the Serious Crime Act 2007) or in accordance with arrangements made by an anti-fraud organisation. The processing of any data so disclosed is permitted.
- 560 Paragraph 12 permits processing of special categories of data which is necessary for the purposes of making a disclosure in good faith under section 21CA of the Terrorism Act 2000

(terrorist financing and identifying terrorist property) or section 339ZB of the Proceeds of Crime Act 2002 (money laundering).

- 561 Paragraph 13 permits processing of special categories of data required to discharge functions involving the provision of services such as confidential counselling and advice in circumstances where the processing is necessary for reasons of substantial public interest and the consent of the data subject is not obtained for one of the specified reasons set out in sub-paragraph (2).
- 562 Paragraph 14 permits processing of data concerning health in certain insurance scheme contexts where details of particular relatives of the principal insured or member are required (e.g. health details of relatives used to calculate the life expectancy of the insured) and the processing can reasonably be carried out without the consent of those relatives. The data controller or data processor must not process these data to make decisions or take actions with respect to those relatives, nor if he is aware of the relative withholding his or her consent to the processing.
- 563 Paragraph 15 permits the processing of special categories of data which is necessary to provide insurance cover for groups without needing explicit consent from each group member. This would include travel, motor or health insurance. Processing is permitted where it is necessary for a contract which satisfies section 7(1)(a) to (c) of the Consumer Insurance (Disclosure and Representations) Act 2012 (group insurance contracts) or a contract to which section 8 of that Act applies (consumer insurance contract for life insurance on the life of another). Third party data processing can be carried out without consent if the controller or processor cannot reasonably obtain the consent of the data subject, and the controller or processor is not aware of the data subject withholding consent to the processing.
- 564 Paragraph 16 permits processing of special categories of data in certain occupational pension scheme contexts and the processing can reasonably be carried out without the consent of the data subject. The data controller or processor must not process personal data to make decisions or take actions with respect to the data subject nor if he or she is aware of the data subject withholding their consent to the processing.
- 565 Paragraph 17 permits the processing of data revealing political opinions by persons or organisations included in the register under section 23 of the Political Parties, Elections and Referendums Act 2000, provided such processing does not cause substantial damage or substantial distress to a person. The processing must be necessary for the purpose of the person or organisation's political activities, which include political campaigning, fund-raising, political surveys and casework. An individual can give notice in writing to the controller requiring the controller to cease processing his or her data, and the controller must cease processing within a reasonable period.
- 566 Paragraph 18 permits processing of special categories of data by elected representatives responding to requests where it is carried out by an elected representative or a person acting with his or her authority. The processing must be in connection with the discharge of the functions of the elected representative and the condition is only met if the processing must be carried out without the data subject's consent for one of the reasons specified in sub-paragraph (2). "Elected representative" is defined in sub-paragraph (3).
- 567 Paragraph 19 permits the disclosure of special categories of data to an elected representative or a person acting with the authority of such a representative and the processing must be carried out without the data subject's consent for one of the reasons specified in sub-paragraph (2).
- 568 Paragraph 20 allows the processing of special categories of data about a prisoner, including information relating to the prisoner's release from prison, for the purpose of informing a

member of the House of Commons or a member of the Scottish Parliament about the prisoner and arrangements for the prisoner's release. The member must be under an obligation not to further disclose the data.

569 Paragraph 21 permits bodies who are responsible for monitoring or eliminating doping in a sport or sporting event, to process special categories of data for those purposes.

Part 3 - Conditions for processing relating to criminal convictions etc

570 Paragraph 22 permits processing of personal data relating to criminal convictions etc. if the data subject has given his or her consent.

571 Paragraph 23 permits processing of personal data relating to criminal convictions etc. where necessary to protect an individual's vital interests and if the data subject is physically or legally incapable of giving consent.

572 Paragraph 24 permits processing of personal data relating to criminal convictions etc. for legitimate activities by not-for-profit bodies with a political, philosophical, religious or trade union aim. The processing must relate to members or former members of that body or to persons who have regular contact with it. Personal data must not be disclosed outside that body without consent from the data subject.

573 Paragraph 25 permits processing of personal data relating to criminal convictions etc. of personal data that has been put in the public domain by the data subject.

574 Paragraph 26 permits processing of personal data relating to criminal convictions etc. necessary for the establishment, exercise or defence of legal claims and when courts are acting in their judicial capacity. As a matter of European Union law, references to "court" will include certain tribunals.

575 Paragraph 27 permits processing of personal data about a conviction or caution necessary for the administration of an account used in the commission of indecency offences involving children. The additional safeguards in Part 4 apply to this processing.

576 Clause 9(4) and (5) have the effect that processing of criminal convictions etc. data is permitted under relevant conditions in Parts 1, 2 and 3 of the Schedule. Since there is no requirement for processing under Article 10 of the GDPR to be in the substantial public interest, paragraph 28(1)(a) disapplies this express requirement where it exists in Part 2 for the purposes of processing criminal convictions etc. data. Paragraph 28(1)(b) applies the additional safeguards in Part 4 to any processing of criminal convictions etc. data under a condition in Part 3.

Part 4 - Additional Safeguards

577 The GDPR requires that processing of special categories of data or criminal convictions etc. data should only be carried out if safeguards for the fundamental rights of the data subject are provided for. The safeguards in this Part apply to processing carried out under paragraph 1 of Schedule 1, Part 2 of Schedule 1, and paragraphs 27 and 28 of Schedule 3 and apply in addition to any express safeguards that are required under any specific processing condition.

578 Paragraph 30 requires the data controller to have an appropriate policy document in place. The controller must have a document which explains the controller's procedures for securing compliance with the principles in Article 5 of the GDPR and explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the condition, with an indication of how long the personal data is likely to be retained.

579 Paragraph 31(1) provides that the controller must, during the relevant period, keep the policy document under review and updated and must make it available to the Commissioner on request.

580 Paragraph 31(2) defines the ‘relevant period’ for the purposes of paragraph 31(1) as beginning when the controller starts to carry out processing of personal data in reliance on a processing condition in Schedule 1 and ending 6 months from the date the controller ceases to carry out such processing.

581 Paragraph 32 requires that a record maintained by the controller, or the controller’s representative, under Article 30 of the GDPR in respect of processing in reliance on paragraph 1 of Schedule 1, Part 2 of Schedule 1, and paragraphs 27 and 28 of Schedule 1 must include information on: which condition is relied on; how the processing satisfies Article 6 of the GDPR and whether the personal data is retained and erased in accordance with the appropriate policy document and if not, the reasons for not following those policies.

Schedule 2: Exemptions etc from the GDPR

Part 1 - Adaptations and restrictions based on Articles 6(3) and 23(1) of the GDPR

582 Paragraph 1 sets out the GDPR provisions restricted or adapted by the exemptions in this Part, the ‘listed GDPR provisions’.

583 Paragraph 2 restricts the application of the listed GDPR provisions to personal data processed for crime and taxation purposes, to the extent that the processing would be likely to prejudice those purposes. Sub-paragraphs (2) and (3) make provision relating to the further processing of personal data collected for the crime and taxation purposes.

584 Paragraph 3 applies where personal data is processed for the crime and taxation purposes by a data controller who is a public body and the restrictions are necessary for the smooth running of a risk assessment system. It restricts a more limited set of GDPR provisions.

585 The crime and taxation restrictions in paragraphs 2 and 3 replicate section 29 of the 1998 Act.

586 Paragraph 4 restricts the application of the listed GDPR provisions to personal data processed for the purposes of the maintenance of effective immigration control, or the investigation or detention of activities that would undermine the maintenance of effective immigration control, to the extent that the processing would be likely to prejudice those purposes. Sub-paragraphs (2) and (3) make provision relating to the further processing of personal data for the immigration purposes.

587 Paragraph 5(1) restricts the application of the listed GDPR provisions to the processing of data protection where the data controller is obliged, under an enactment, to disclose personal data to the public, to the extent the application of those provisions would prevent compliance with that obligation. This is based on the exemption under section 34 of the 1998 Act.

588 Paragraph 5(2) and (3) restrict the listed GDPR provisions where the disclosure of personal information is required by law or necessary for the purpose of or in connection with legal proceedings. They replicate the exemptions under section 35 of the 1998 Act.

Part 2 - Restrictions based on Article 23(1): General

589 Paragraph 6 sets out the listed GDPR provisions restricted by the exemptions in this Part.

590 Paragraph 7 restricts the application of the listed GDPR provisions to personal data processed for the purposes of discharging the functions concerned with the protection of members of the public, charities and fair competition in business, as set out in the table.

591 Paragraph 8 restricts the application of the listed GDPR provisions to personal data processed for the purposes of discharging regulatory functions relating to legal services, the health service and children’s services.

592 Paragraph 9 restricts the application of the listed GDPR provisions to personal data processed for the purposes of statutory functions relating to the oversight of public bodies, as specified in the table.

593 The restrictions in paragraphs 7, 8 and 9 apply to the extent that the processing would be likely to prejudice the proper discharge of those functions. They are based on the exemptions provided for under section 31 of the 1998 Act.

594 Paragraph 11 restricts the application of the listed GDPR provisions to personal data processed for the purposes of avoiding an infringement of parliamentary privilege. This replicates section 35A of the 1998 Act.

595 Paragraph 12(1) restricts the listed GDPR provisions to personal data processed for the purposes of determining a person's suitability for judicial office or Queen's Counsel.

596 Paragraph 12(2) restricts the listed GDPR provisions to personal data processed by an individual acting in a judicial capacity or a court or tribunal acting in its judicial capacity. Paragraph 12(3) restricts the listed GDPR provisions in relation to all other personal data to the extent the application of those provisions would be likely to prejudice judicial independence or judicial proceedings. This ensures the administration of justice is not undermined by the application of the GDPR.

597 Paragraph 13 restricts the application of the listed GDPR provisions to personal data processed for the purposes of conferring Crown honours, or for the purposes of assessing a person's suitability for the offices listed in sub-paragraph (2). The Secretary of State may, by regulations, amend that list. Regulations are subject to the affirmative procedure.

Part 3 - Restrictions based on Article 23(1) in other circumstances

598 Paragraphs 14 and 15 provide that a data controller is not obliged to disclose information under Article 15 of the GDPR if to do so would mean disclosing information relating to another individual who can be identified from the information, except where there the other individual has consented; or it is reasonable in all circumstances to comply with the request without that individual's consent. This retains the effect of sections 7(4), (5), (6) and 8(7) of the 1998 Act.

Part 4 - Restrictions based on Article 23(1): Restrictions of Rules in Articles 13 to 15

599 Paragraph 16 sets out the listed GDPR provisions restricted by the exemptions in this Part.

600 Paragraph 17 restricts the application of the listed GDPR provisions to personal data that consists of material over which legal privilege (or in Scotland, confidentiality in communications) can be claimed or maintained in legal proceedings. It replicates the exemption in paragraph 10 of Schedule 7 to the 1998 Act.

601 Paragraph 18 restricts the obligation to comply with the listed GDPR provisions to the extent that compliance would result in self-incrimination. It also provides that information disclosed by a person in compliance with Article 15 is not admissible against the person in proceedings for an offence under Parts 5 or 6 of the Bill. This replicates the exemption in paragraph 11 of Schedule 7 to the 1998 Act.

602 Paragraph 19 restricts the application of the listed GDPR provisions to personal data processed for the purposes of, or in connection with, a corporate finance to the extent that one of the conditions set out in that paragraph is met. This restriction is based on the exemption for this purpose under paragraph 6 of Schedule 7 to the 1998 Act and the Data Protection (Corporate Finance Exemption) Order 2000 (SI 2000/ 184).

- 603 Paragraph 20 restricts the application of the listed GDPR provisions to personal data processed for management forecasting or management planning purposes, to the extent the application of those provisions would prejudice the conduct of the business or activity concerned. This replicates the exemption for this purpose under paragraph 5 of Schedule 7 to the 1998 Act.
- 604 Paragraph 21 restricts the application of the GDPR listed provisions to personal data that consists of the data controller's record of his or her intentions in relation to any negotiations with the data subject, to the extent that the application of those provisions would be likely to prejudice the negotiation. Paragraph 21 replicates the exemption for this purpose under paragraph 7 of Schedule 7 to the 1998 Act.
- 605 Paragraph 22 restricts the application of the GDPR listed provisions to personal data consisting of a confidential reference given (or to be given) by the controller for education and employment purposes. This replicates the exemption for those purposes in paragraph 1 of Schedule 7 to the 1998 Act.
- 606 Paragraph 23 restricts the listed GDPR provisions where personal data consists of information recorded by candidates during an exam. It also modifies the time limits for complying with disclosure obligations under Article 15, where the personal data to be disclosed consists of examination marks or other information processed for the purposes of determining the results of an exam. This ensures candidates cannot obtain their exam marks they are first published and replicates the exemption for those purposes under paragraphs 8 and 9 of Schedule 7 to the 1998 Act.

Part 5 - Exemptions etc based on Article 85(2) for reasons of freedom of expression and information

- 607 This Part provides that certain GDPR provisions will not apply when personal data is being processed with a view to publication only for one or more special purpose(s) (as defined in paragraph 24(8)), the controller reasonably believes that the publication would be in the public interest and also that the application of any of the listed GDPR provisions would be incompatible with the special purposes.
- 608 Paragraph 24(2) to (4) set out what factors the controller must take into consideration when considering whether publication would be in the public interest, including whether guidance on such matters is covered in any relevant codes of practice listed in paragraph 24(4).
- 609 Paragraph 24(5) to (6) allows the Secretary to amend the list of specified codes of practice listed in paragraph 24(4) through the affirmative resolution procedure.
- 610 Paragraph 24(7) lists the GDPR provisions which do not apply when personal data is being processed only for one of more of the special purposes.
- 611 Paragraph 24(9) defines the meaning of 'publish' for the purposes of this Schedule.

Part 6 - Derogations etc based on Article 89 for research, statistics and archiving

- 612 This Part restricts the application of the listed GDPR provisions to personal data processed for scientific or historical research purposes, statistical purposes or archiving in the public interest from specified provisions in the GDPR relating to data subjects' rights where this would prevent or seriously impair achievement of those purposes and the relevant safeguards are met.
- 613 Paragraph 25 applies where personal data is processed for scientific or historical research and statistical purposes. The safeguards are that the data is processed in accordance with Article 89(1), as supplemented by clause 18, and the results of research or any resulting statistics are not made available in a form which identifies the data subject.

614 Paragraph 26 applies where personal data is processed for archiving purposes. The safeguards are that the data is processed in accordance with Article 89(1), as supplemented by clause 18.

Schedule 3: Exemptions etc from the GDPR: health, social work, education and child abuse

615 This Schedule makes provision for restrictions from certain GDPR provisions where this is necessary for health, education and social work purposes. It seeks to preserve the substance of the orders made under section 30 of the 1998 Act:

- The Data Protection (Subject Access Modification) (Health) Order 2000 [SI 2000/ 413]
- The Data Protection (Subject Access Modification)(Social Work) Order 2000 [SI 2000/ 415], and
- The Data Protection (Subject Access Modification)(Education) Order 2000 [SI 2000/ 414].

616 Part 1 sets out the listed GDPR provisions restricted by the exemptions in this Schedule.

617 Part 2 restricts the application of the listed GDPR provisions in relation to health information. Restrictions apply where:

- the application of the listed GDPR provisions would be likely to cause serious harm to the physical or mental condition of the data subject, or any other person;
- information is processed by a court and consists of information supplied in a report or other evidence given to the court by certain bodies; or
- a request is made on behalf of the data subject by the person with parental responsibility for the data subject or by the person appointed by the court to manage his or her affairs would result in disclosure of information contrary to the data subject's expectations and wishes.

618 Part 3 restricts the application of the listed GDPR provisions in relation to social work information. The restrictions apply to personal data processed by a range of authorities or bodies pursuant to specified social services functions and by the courts in children's and family proceedings. Restrictions apply where:

- the application of the listed GDPR provisions would be like be likely to cause serious harm to the physical or mental health of the data subject or any other person;
- the information has been provided to a court and the court may withhold from the data subject; and
- a request is made on behalf of the data subject for information the data subject has expressly indicated should not be disclosed.

619 Part 4 restricts the application of the listed GPDR provisions in relation to educational information Restrictions apply where:

- the data has been provided to a court in certain proceedings and it is information that the court may withhold from the data subject;
- exercise of the right would be likely to cause serious harm to the physical or mental health or condition of the data subject or any other person.

620 Part 5 restricts the application of Articles 13(1) to (3), 14(1) to (4) and 15(1) to (3) to the processing of personal data consisting of information as to whether the data subject is or has been the subject of or may be at risk of child abuse, to the extent it would not be in the best interests of the data subject to apply those provisions.

Schedule 4: Exemptions etc from the GDPR: Disclosure prohibited or restricted by an enactment

621 This Schedule seeks to preserve to the substance of the Data Protection (Miscellaneous Subject Access Exemptions) Order 2000 [SI 2000/419].

622 The Schedule restricts the application of the listed GDPR provisions to personal data consisting of information which is prohibited to be disclosed under specified enactments for the purposes of safeguarding the interests of the data subject or the rights and freedoms of others.

623 The personal data which are restricted under this schedule relate to human fertilisation and embryology information; information contained in adoption and parental order records and reports, and statements and records of the special educational needs of children in England or Wales, Scotland and Northern Ireland; and, in Scotland only, information provided by reporters for the purposes of a children's hearing.

Schedule 5: Accreditation of certification providers: reviews and appeals

624 This Schedule sets out the process by which applicants can request that accreditation authorities review decisions taken concerning their accreditation as a certification authority.

625 Paragraph 2 sets out the conditions for review, including the form in which a request must be made, the time period for making such a request and the nature of information which must be provided. It also requires the accreditation authority to review the decision and inform the applicant of the outcome.

626 Paragraph 3 sets out the right for applicants to appeal a review decision by the accreditation authorities and the manner in which it must make or discontinue an appeal.

627 Paragraph 4 specifies the manner in which an appeal panel must be formed, including the specific requirements for appeals against decisions taken by the Commissioner or the national accreditation body.

628 Paragraph 5 specifies how an appeal hearing must be held, if necessary.

629 Paragraph 6 sets out the timing and manner in which an appeal panel must make its recommendation and communicate its final decision.

Schedule 6: The applied GDPR and applied Chapter 2

630 This Schedule specifies how the GDPR provisions will apply to areas outside the scope of Union law. In line with Article 2(2) of the GDPR, the Regulation only applies to the processing of data in the course of an activity which is subject to Union law. This Schedule makes the necessary modifications to the provisions to reflect the application to non-Union law activities, creating an applied GDPR. These provisions describe how Union law references should be interpreted in the domestic context.

631 Paragraph 2 explains that unless otherwise specified, references in this Schedule to "this Regulation" and to provisions of the GDPR, refer to the applied GDPR.

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

- 632 Paragraph 3 specifies how references to “Union law”, “Member State Law”, “the law of a Member State”, and “Union or Member State law” should be regarded as meaning domestic law, unless exceptions apply. Paragraph 3(2) explains the definition of “domestic law”.
- 633 Paragraph 4 specifies how references to “the Union”, a “member state” and “member states” should be regarded as meaning the United Kingdom unless otherwise specified.
- 634 Paragraph 5 specifies how references to a “supervisory authority”, “Competent supervisory authority” or “supervisory authorities” should be regarded as meaning the Commissioner unless otherwise specified.
- 635 Paragraph 6 specifies how certain provisions in Chapter 1 should be interpreted, unless otherwise specified, when the processing concerned is outside the scope of Union law.
- 636 Paragraph 8 in the context of Article 3 (territorial application) omits references to “subject to subsection (3)”, “subject to subsection (4)”, “or section 57(8) or 103(3) of this Act (processor to be treated as controller in certain circumstances”).
- 637 Paragraph 9 in the context of Article 4 of the GDPR, (definitions) makes clear that references to “Commissioner” should be regarded as the Information Commissioner, makes reference “binding corporate rules on the territory of a Member State” be regarded as the United Kingdom.
- 638 Paragraph 10 in the context of Article 6 of the GDPR, determining the lawfulness of processing, makes clear that it is for the Secretary of State to determine, with references to “Member States” and “Union or Member State law” substituted for domestic ones.
- 639 Paragraph 11 in the context of Article 8 of the GDPR, a child’s consent to accessing relevant services, makes clear that the conditions are subject to this Bill and domestic law, rather than the “general contract law of Member States”.
- 640 Paragraph 12 in the context of Article 9 of the GDPR (processing special categories of personal data) removes the reference to “Union or Member State law”, substitutes “Union or Member State law” with domestic equivalents and substitutes references to public interest, healthcare contracts, professional secrecy, archiving purposes, and national competent bodies in the Union Law or Member State context, with references to this Bill.
- 641 Paragraph 13 in the context of processing of personal data relating to criminal convictions, makes clear that the relevant safeguards are drawn from this Bill, rather than Union or Member State law.
- 642 Paragraph 14 in the context of exercising a data subject’s rights, references to “supervisory authority” are substituted for the domestic “Commissioner”. The reference to the “Commission’s power”, as in European Commission, is removed.
- 643 Paragraph 15 in the context of Article 13 of the GDPR, providing information to a data subject where data has been collected about them, removes the reference to the “controller’s representative” and makes clear that the reference to the “supervisory authority” means the Commissioner.
- 644 Paragraph 16 in the context of Article 14 of the GDPR, providing information to a data subject where data has not been collected about them, removes the reference to the “controller’s representative”, makes clear that the reference to the “supervisory authority” means the Commissioner, and that the relevant law applying here is domestic.
- 645 Paragraph 17 in the context of Article 17 of the GDPR, right of erasure, makes clear that references to Union or Member State law are substituted with domestic ones.

- 646 Paragraph 18 in the context of Article 18 of the GDPR, right to restrictions of processing, makes the reference to the “of the Union or Member State Law” means the United Kingdom.
- 647 Paragraph 19 removes the reference to Article 21 of the GDPR, paragraph 5 “and notwithstanding Directive 2002/58/EC”.
- 648 Paragraph 20 in the context of Article 22 of the GDPR, automated individual-decision making, including profiling substitutes “qualifying significant decision” for the purpose of section 13 of the 2017 Act.
- 649 Paragraph 21 in the context of Article 23 of the GDPR, restrictions removes references to the “Union or Member State law to which the data controller or processor is subject” and replaces it with “In addition to the provisions made by section 14 of and Schedules 2, 3 and 4 to the 2017 Act, the Secretary of State”, makes clear that the reference to “of the Union or of a Member State” means the “United Kingdom”.
- 650 Paragraph 22 in the context of Article 26 of the GDPR (joint processor), makes clear that references to Union or Member State law to which controllers are subject should be substituted with domestic law.
- 651 Paragraph 23 removes the reference to Article 27 of the GDPR “representatives of controllers or processors not established in the Union”.
- 652 Paragraph 24 in the context of Article 28 of the GDPR, (processor), makes clear that references to Union or Member State law should be substituted with domestic ones.
- 653 Paragraph 25 in the context of Article 30 of the GDPR (records of processing activities), removes references to the “controller’s representative” and makes clear that records must be made available to the UK authority (the Commissioner) on request, rather than a Union body.
- 654 Paragraph 26 in the context of Article 31 of the GDPR (cooperation with the supervisory authority), makes clear that the controller and processor must cooperate with the Commissioner on request, rather than a Union body.
- 655 Paragraph 27 in relation to Article 35 of the GDPR (data protection impact assessment) omits paragraphs 4, 5, 6 and 10.
- 656 Paragraph 28 in the context of Article 36 of the GDPR (prior consultation), makes clear that references to a “supervisory authority” mean the Commissioner. Also that it is for the (domestic) “Secretary of State” rather than the “Member States” to make a relevant decision.
- 657 Paragraph 29 in the context of Article 37(7) of the GDPR, designation of the data protection officer, makes clear that references to a “supervisory authority” mean the Commissioner.
- 658 Paragraph 30 in the context of Article 39(1) of the GDPR, tasks of the data protection officers, makes clear that references to “Union or Member State data protection provisions” are substituted with domestic ones, and makes clear that references to a “supervisory authority” mean the Commissioner.
- 659 Paragraph 31 in the context of Article 40 of the GDPR, codes of conduct, and makes clear that references to a “supervisory authority” mean the Commissioner, and that it is for the Commissioner to register and publish the code, rather than a Union body.
- 660 Paragraph 32 in the context of Article 41 of the GDPR, monitoring of approved codes of conduct, and makes clear that references to “the competent supervisory authority” mean the Commissioner.
- 661 Paragraph 33 in the context of Article 42 of the GDPR, certification, makes clear that references to “Union or Member State” authority, are substituted with the Commissioner, and that certification is for the Commissioner or other relevant certification bodies.

- 662 Paragraph 34 in the context of Article 43 of the GDPR, certification bodies, makes clear that references to “Union or Member State” law or authority, or certification bodies, are substituted with the Commissioner and relevant domestic law or bodies. It also removes the Commission’s power to adopt delegated or implementing acts.
- 663 Paragraph 35 in the context of Article 45 of the GDPR, transfers on the basis of an adequacy decision, makes clear that relevant decisions are made in accordance with Article 45 of the GDPR, and that those decisions should not have been repealed or suspended.
- 664 Paragraph 36 in the context of Article 46 of the GDPR, transfers subject to appropriate safeguards, makes clear that relevant decisions are made in accordance with Article 45 of the GDPR, that references to the “supervisory authority” mean the Commissioner, and that decisions made by the Commissioner under the 1998 Act continue to have effect unless revoked by the Commissioner.
- 665 Paragraph 37 in the context Article 47 of the GDPR, binding corporate rules, makes clear that approval is for the Commissioner, and that references to “the competent courts of the Member States” mean “a court” and reference to “on the territory of a Member State” should mean in the “United Kingdom”.
- 666 Paragraph 38 in the context of Article 49 of the GDPR, derogations for specific situations, makes clear that such a decision relates to Article 45(3) of the GDPR, that the reference to “the competent supervisory authority” means the Commissioner; that the public interest relates to domestic law and is subject to the relevant section 17(1) of this and that paragraph 1 of Article 49 of the GDPR is subject to domestic law, through 17(2) of this Act.
- 667 Para 39 in the context of Article 50 of the GDPR, international co-operation for the protection of personal data, makes clear that references to the “Commission and competent supervisory authorities” mean the Commissioner.
- 668 Paragraph 40 in the context of Article 51 of the GDPR, supervisory authority, makes clear that references to “Member State” should be the Commissioner, in determinations about independent public authorities.
- 669 Paragraph 41 in the context of Article 52 of the GDPR, independence, makes clear that references to the “supervisory authority” and relevant powers or tasks, mean the Commissioner.
- 670 Paragraph 42 removes Article 53 of the GDPR, general conditions for the members of the supervisory authority.
- 671 Paragraph 43 removes Article 54 of the GDPR, rules on the establishment of the supervisory authority.
- 672 Paragraph 44 in the context of Article 55 of the GDPR, competence, removes the reference to territory of “Member State”.
- 673 Paragraph 45 removes Article 56 of the GDPR, competence of the lead supervisory authority.
- 674 Paragraph 46 in the context of Article 57 of the GDPR, tasks, makes clear that references to the “supervisory authorities” mean the Commissioner, and makes clear that the relevant territory is the United Kingdom and removes references to other “supervisory authorities”.
- 675 Paragraph 47 in the context of Article 58 of the GDPR, powers, makes clear that references to the “supervisory authorities” mean the Commissioner, removes the reference to the controller or processor’s representative and substitutes “Union or Member State procedural law” or the “Charter” with “domestic law”.

- 676 Paragraph 48 in the context of Article 59 of the GDPR, activity reports, makes clear references to “the Government and other authorities as designated by Member State law” mean the Secretary of State.
- 677 Paragraph 49 applies Chapter VII to Articles 60 to 76 of the GDPR with a replacement Article (new Article 61). This Article explains how the Commissioner can cooperate with other supervisory authorities, and how the Commissioner should have regard to the activities of the European Data Protection Board, and any implementing acts adopted by the Commission under Article 67 (exchange of information).
- 678 Paragraph 50 modifies Article 77 of the GDPR which deals with the right to lodge a complaint with the supervisory authority.
- 679 Paragraph 51 modifies Article 78 of the GDPR which deals with the right of a person to seek a judicial remedy against a supervisory authority. References to the decisions of the supervisory authority are to be read as those of the Commissioner. Paragraph 2 and replace with 3 – “Proceedings against the Commissioner are to be brought before a court in the United Kingdom” of Article 78 of the GDPR are omitted because they are not relevant to processing covered by Part 2, Chapter 3 of the Bill.
- 680 Paragraph 52 modifies Article 79 which provides data subjects with a right to an effective judicial remedy against a controller or processor, in addition to having the right to lodge a complaint with the supervisory authority. Paragraph 2 is replaced with “Proceedings against a controller or a processor are to be brought before a court (see section 167 of the 2017 Act)”.
- 681 Paragraph 53 omits from Article 80, representation of data subjects, where provided for by Member State law” from paragraph 1 and paragraph 2.
- 682 Paragraph 54 modifies Article 81 of the GDPR which is concerned with the suspension of court proceedings. The modification would allow courts in the United Kingdom to suspend proceedings if they found that a case involving the same subject matter involving the same data controller or processor was pending in another court or tribunal.
- 683 Paragraph 55 modifies Article 82 of the GDPR which is concerned with the right to compensation and liability.
- 684 Paragraph 56 modifies Article 83 of the GDPR which sets out general conditions for a supervisory authority imposing administrative fines. References to the ‘supervisory authority’ are replaced with the ‘Commissioner’ and references to ‘Member States’ laying down rules on whether and to what extent administrative fines can be imposed are replaced by the ‘Secretary of State’.
- 685 Paragraph 57 modifies Article 84 on penalties. Paragraph 1 has been replaced by “rules on other penalties applicable to infringements of this Regulation are set out in the 2017 Act (see in particular Part 6 (enforcement)).” and omits paragraph 2.
- 686 Paragraph 58 in the context of Article 85 of the GDPR, processing and freedom of expression and information, makes clear that references to “Member States shall”, mean “Secretary of State may”.
- 687 Paragraph 59 replaces reference to Union or Member State law to which the public authority or body is subject in Article 86 of the GDPR, with domestic law.
- 688 Paragraph 60 removes Article 88 (processing in the context of employment).
- 689 Paragraph 61 removes article 88 of the GDPR, processing in the context of employment.

690 Paragraph 62 in the context of Article 89 of the GDPR, safeguards and derogations relating processing for archiving purposes etc, makes clear that references to “Union or Member State law” mean “the Secretary of State”.

691 Paragraph 63 removes Article 90 of the GDPR, obligations of secrecy.

692 Paragraph 64 removes Article 91 of the GDPR, existing data protection rules of churches and religious associations.

693 Paragraph 65 removes Article 92, exercise of the delegation.

694 Paragraph 66 removes **Article 93, committee procedure**.

695 Paragraph 67 removes **Article 94, repeal of Directive 95/46/EC**.

696 Paragraph 68 removes Article 95, relationship with Directive 2002/58/EC.

697 Paragraph 69 modifies Article 96 on the relationship with previously concluded Agreements. References to “Member States” should mean the United Kingdom or the Commissioner.

698 Paragraph 70 removes Article 97, Commission reports.

699 Paragraph 71 removes Article 98, Commission reviews.

700 Paragraph 72 removes Article 99, entry into force and application.

Schedule 7: Competent authorities

701 This Schedule sets out a list of the competent authorities, meaning any United Kingdom Government department other than a non-ministerial Government department.

Schedule 8: Conditions for sensitive processing

702 This Schedule sets out the conditions for sensitive processing under specific circumstances. These include judicial and statutory purposes, protecting individuals’ vital interests, personal data in the public domain, legal claims and judicial acts, prevention of fraud, archiving and circumstances specified in regulation made by the Secretary of State.

Schedule 9: Conditions relevant for purposes of the first principle: any processing

703 This Schedule sets out the relevant conditions for the lawful processing of sensitive personal.

Schedule 10: Conditions relevant for purposes of the first principle: sensitive processing

704 This Schedule sets out the relevant conditions for lawful and fair sensitive processing.

Schedule 11: Other exemptions

705 This Schedule provides for exemptions to:

- the data protection principles set out in Part 4 of the Bill, except where they require compliance with condition that the processing is lawful, as set out in clause 84(1)(a) and the conditions in Schedules 9 and 10,
- the rights of data subjects, and
- the need to communicate a personal data breach to the Commissioner.

- 706 Paragraph 2 provides an exemption in relation to the prevention of crime.
- 707 Paragraph 3 provides exemptions in relation to disclosures required by law or in connection with legal proceedings or obtaining legal advice.
- 708 Paragraph 4 provides an exemption in relation to Parliamentary privilege.
- 709 Paragraph 5 provides an exemption in relation to judicial proceedings.
- 710 Paragraph 6 provides exemptions in relation to Crown honours and dignities.
- 711 Paragraph 7 provides exemptions in relation to the any prejudice to the combat effectiveness of the armed forces.
- 712 Paragraph 8 provides exemptions in relation to circumstances likely prejudice of the economic wellbeing of the United Kingdom.
- 713 Paragraph 9 provides exemptions in relation to legal professional privilege.
- 714 Paragraph 10 provides exemptions in relation to negotiations.
- 715 Paragraph 11 provides exemptions in relation to confidential references given by the controller.
- 716 Paragraph 12 provides exemptions in relation to exam scripts and marks.
- 717 Paragraph 13 provides exemptions in relation to research and statistics. This exemption is only available where there are appropriate safeguards and the results of the research will not be made available in a form that identifies a data subject.
- 718 Paragraph 14 provides exemptions in relation to archiving in the public interest. This exemption is only available where the processing is subject to appropriate safeguards.

Schedule 12: The Information Commissioner

- 719 This Schedule seeks to replicate Schedule 5 to the 1998 Act and includes details about the Commissioner's term of office.
- 720 Paragraph 1 provides that the Commissioner will continue to be a corporation sole and independent of Government.
- 721 Paragraph 2 includes details about the appointment process and length of tenure. The Commissioner can only be appointed on the basis of merit following an open and fair competition.
- 722 Paragraph 3 provides details about how the Commissioner may resign or be removed from office.
- 723 Paragraph 4 includes details about the Commissioner's pay and pension.
- 724 Paragraph 5 allows the Commissioner to appoint deputy commissioners and other staff, having regard to the principles of open and fair competition, and includes provision about their pay and pensions.
- 725 Paragraph 6 sets the conditions for an officers and staff to carry the Commissioner's functions, in the Commissioner's absence.
- 726 Paragraph 7 specifies how the Commissioner's seal is to be authenticated.
- 727 Paragraph 8 provides that a document purporting to be issued by the Commissioner can be received in evidence unless the contrary is shown.

728 Paragraph 9 is self-explanatory.

729 Paragraph 10 specifies where fees collected by the Commissioner in the course of carrying out the Commissioner's functions should be paid.

730 Paragraph 11 requires the Commissioner to keep proper records of accounts and prepare a report for each financial year for scrutiny by the Comptroller and Auditor General.

731 Paragraph 12 disapplies certain provisions in this Schedule in relation to Scotland.

Schedule 13: Other general functions of the Commissioner

732 This Schedule sets out other functions of the Commissioner. This includes to:

- monitor and enforce Parts 3 and 4 of the Bill. Part 2 is linked to the GDPR and so no specific reference is required;
- promote public awareness and understanding;
- advise Parliament, the Government and other institutions regarding the processing and protection of personal data;
- promote awareness of controllers and processors of their obligations;
- provide information concerning data subject rights and cooperate with supervisory and foreign designated authorities;
- cooperate with Law Enforcement Directive (LED) supervisory authorities and foreign designated bodies to ensure consistency of approach and sharing information and mutual assistance;
- conduct investigations on the application of Parts 3 and 4 of this Bill;
- monitor developments that impact on the protection of personal data; and
- contribute to the activities of the European Data Protection Board.

733 This Schedule also provides the Commission with general powers to investigate, correct, authorise and advise on powers relating to personal data. This includes notifying controllers or processors of infringements, issue warnings on infringements, issue reprimands, issue opinions to Parliament or Government, or other relevant bodies.

Schedule 14: Cooperation and mutual assistance

734 This Schedule sets out how the Commissioner will co-operate with LED supervisory authorities and foreign designated authorities to ensure consistent application and enforcement of the Law Enforcement Directive and compliance with the Data Protection Convention.

735 An "LED supervisory authority" is a supervisory authority in an EEA state other than the UK responsible for Article 41 of the Law Enforcement Directive.

736 A "foreign designated authority" is an authority, in a state other than the UK and which is bound by the Data Protection Convention, responsible for the Data Protection Convention.

737 Part 1 of the Schedule sets out the functions of the Commissioner with respect to Article 50 of the Law Enforcement Directive which states that LED supervisory authorities must provide each other with relevant information and mutual assistance in order to implement and apply the Directive consistently.

- 738 Paragraph 1(1) states the Commissioner may provide information or assistance to the European Commission and an LED supervisory authority that is necessary for the performance of their functions relating to the protection of individuals with respect to the processing of personal data.
- 739 Paragraph 1(2) states the Commissioner may ask an LED supervisory authority to provide information or assistance that is required for the performance of the Commissioner's data protection relating to the protection of individuals with respect to the processing of personal data.
- 740 Paragraph 2 sets out how the Commissioner should respond to a request from an LED supervisory authority for information or assistance.
- 741 Paragraph 3 sets out that any information or assistance must be provided free of charge, but the Commissioner may in exceptional circumstances have an agreement with an LED supervisory authority to indemnify themselves for specific expenditure arising from providing information or assistance. Clause 129 (Fees) of the Bill sets out the power for the Commissioner to charge a fee for other services.
- 742 Paragraph 4 states that information received by the Commissioner from an LED supervisory authority must only be used for the purposes specified in the original request.
- 743 Part 2 of the Schedule sets out the functions of the Commissioner with respect to Article 13 of the Data Protection Convention and cooperating with foreign designated authorities. This replaces the provision of the Data Protection (Functions of Designated Authority) Order 2000 (SI 186/2000).
- 744 Paragraph 6 states the Commissioner must take appropriate measures to provide information, relating to law and administrative practice in the field of data protection and the processing of personal data in the UK, when requested by foreign designated authorities. The Commissioner can request the same information from foreign designated authorities.
- 745 Paragraphs 7 and 8 concern how the Commissioner deals with requests for assistance to enable a persons resident either in or outside the UK to exercise their rights under the Data Protection Convention.
- 746 Paragraph 9 states that information received by the Commissioner from a foreign designated authority as a result of request for information may only be used for the purposes specified in the request.

Schedule 15: Powers of entry and inspection

- 747 This Schedule provides clarification around powers of entry and inspection. It substantively replicates Schedule 9 to the 1998 Act.
- 748 Paragraph 1 sets out the circumstances in which a circuit judge or a District Judge (Magistrates' Court) may grant a warrant to the Commissioner other than in connection assessment notices.
- 749 Paragraph 2 gives the court the power to the issue of warrants in connection with assessment notices.
- 750 Paragraph 3 requires the judge to not issue a warrant if the processing is required for special purposes (i.e. for the purposes of journalism or academic, artistic or literary purposes).
- 751 Paragraph 4 provides restrictions and conditions which a Judge must consider and be satisfied have been met before issuing warrant. A Judge may only issue a warrant if satisfied

that one or more of the requirements within paragraph 4, sub-paragraph (1) is met. In order for the requirement under paragraph 4, sub-paragraph (1) to be satisfied, the three conditions within paragraph 4, sub-paragraphs (2) to (4) must be met.

752 Paragraph 5 makes provision as to the content of warrants. A warrant may include the power to enter and search premises and inspect and seize documents.

753 Paragraph 6 sets out the process to be followed by a judge when issuing a warrant.

754 Paragraph 7 allows a person executing a warrant issued under this Schedule to use reasonable force.

755 Paragraph 8 requires that a warrant issued must be executed at a reasonable hour, unless there are grounds to suspect that it would defeat the purpose of the warrant.

756 Paragraph 9 requires the person executing the warrant to show the occupier the warrant and give the occupier a copy. Otherwise it must be left in a prominent place on the premises.

757 Paragraph 10 requires a person executing a warrant to provide a receipt and give the occupier a copy when seizing a document. It does not require the person executing the warrant to provide a copy of the document, if providing a copy would result in undue delay. The seized document may be retained for as long as necessary.

758 Paragraphs 11 and 12 exempt from seizure certain privileged communications.

759 Paragraph 13 makes provision about partially exempt material. It allows the person in occupation of the premises to object to inspection or seizure of materials on the grounds that it is not fully applicable under the powers of the warrant. It requires that the person must, on request, provide a copy of material that is not exempt from the powers of the warrant.

760 Paragraph 14 makes provision relating to the return of warrants.

761 Paragraph 15 sets out offences relating to the execution of a warrant.

762 Paragraph 16 sets out the circumstances in which a statement given in explanation of any document or other material found on the premises in connection with the execution of a warrant may be used in evidence against the person who gave the statement.

763 Paragraph 17 makes provision in relation to means of transport which fall within the definition of “premises” for the purposes of this Schedule and also the meaning of an occupier of premises in that context.

764 Paragraph 18 makes the changes required so this Schedule may apply in relation to Scotland.

765 Paragraph 19 does the same for Northern Ireland.

Schedule 16: Penalties

766 This Schedule makes further provisions in relation to administrative penalties. These provisions are broadly equivalent to the provisions provided in the 1998 Act in regards to monetary penalties.

767 Paragraph 1 defines the meaning of a ‘penalty’.

768 Paragraph 2 explains that the Commissioner must give notice to the data controller or processor that they intend to issue them a penalty notice. The Commissioner cannot issue a penalty notice after six months has passed from the date they issued the written notice.

769 Paragraph 3 explains what the Commissioner must include in the notice of intent to issue a penalty notice. This includes the amount of the penalty, the nature of the offence, the period in

which the controller or processor can make written representations about the Commissioner's intention to issue a penalty notice, and whether a controller or processor can make oral representations.

770 Paragraph 4 states that the Commissioner must first consider any oral or written representations by the controller or processor, before determining whether to give a penalty notice. The Commissioner must wait until after the time allocated for making oral or written statements by the controller or processor has passed before issuing a penalty notice.

771 Paragraph 5 sets out what must be provided in the penalty notice. This may include, for example, reasons why the Commissioner proposes to impose the penalty, reasons for the amount specified and details on rights of appeal.

772 Paragraph 6 provides that any penalty must be paid within a specified period and that period cannot be less than 28 days from the date the penalty notice was issued.

773 Paragraph 7 allows the Commissioner to vary a penalty notice by given written notice and sets out certain requirements for the variation notice.

774 Paragraph 8 outlines the procedure the Commissioner must follow when cancelling a penalty notice.

775 Paragraph 9 provides what conditions must be satisfied before the Commissioner can take to enforce a penalty.

Schedule 17: Relevant records

776 This Schedule explains the meaning of 'relevant records' for the purposes of the offence in clause 171 (prohibition of requirement to produce relevant records).

777 Paragraph 1 makes it clear that relevant records include health records, records relevant to a conviction or a caution and records relating to statutory functions.

778 Records relating to convictions and cautions are defined in paragraph 2. Records relating to statutory functions are defined in paragraph 3.

779 Paragraph 4 sets out the meaning of 'data subject access rights' for the purposes of this Schedule and the offence in clause 171.

780 Paragraph 5 makes it clear that a relevant record can include a statement that a controller is not processing data about an individual in relation to a particular matter.

781 Paragraph 6 provides the Secretary of State with a power to amend this Schedule via the affirmative resolution procedure.

Schedule 18: Minor and consequential amendments

782 This Schedule makes amendments to legislation which are necessary to reflect the repeal of the 1998 Act and the requirements of the GDPR.

783 Paragraph 1 amends the Consumer Credit Act by substituting references to the 1998 Act with references to the GDPR.

784 Paragraph 2 repeals the 1998 Act.

785 Paragraph 3 amends the Immigration and Asylum Act 1999 by substituting references to the 1998 Act with references to the GDPR.

786 Paragraphs 4 to 10 amend the 2000 Act to reflect the provisions of the GDPR.

- 787 In particular, paragraph 6 amends section 40 of the 2000 Act to ensure that personal data is only disclosed in response to FOI requests where this would not breach the GDPR principles at Article 5 GDPR or specified rights of data subjects. When determining whether disclosure would be lawful under Article 5(1)(a) of the GDPR, by applying the first condition at section 40(3A)(a) of the 2000 Act to a request under section 40 of the 2000 Act, paragraph 6(8) allows FOI public authorities to rely on Article 6(1)(f) of the GDPR (legitimate interests) as a basis for processing.
- 788 Paragraph 7 removes the requirement in section 49 of the 2000 Act for the Information Commissioner to publish reports on the operation of that Act. This is no longer needed in the light of clause 135 of this Bill which introduces a general requirement for the Information Commissioner to publish annual reports on his/her functions.
- 789 Paragraph 8 mirrors the provisions on contempt of court in clause 181 of this Bill to ensure they apply to FOI proceedings.
- 790 Paragraph 9 mirrors the provision in clause 127 of this Bill on confidentiality of information. This means that information obtained by the Information Commissioner in connection with investigations under the 2000 Act is covered by the provision.
- 791 Paragraph 10 amends section 77 of the 2000 Act (altering records to prevent disclosure) to remove reference to the subject access provisions under the 1998 Act. The alteration of records to frustrate disclosure following a subject access request is now covered by the offence in clause 164 of this Bill.
- 792 Paragraphs 11 to 13 amend the Freedom of Information (Scotland) Act 2002 to reflect the provisions of the GDPR. The changes are similar to the amendments described above in relation to the 2000 Act.
- 793 Paragraphs 14 to 21 make amendments to the Environmental Information Regulations 2004 and the Environmental Information (Scotland) Regulations 2004 to reflect the terminology of the GDPR and adding specific references to the GDPR principles.
- 794 Paragraph 22 omits sections 77 to 78 of the Criminal Justice and Immigration Act 2008. These sections introduced an order-making power to increase the maximum penalty for the offence of unlawfully obtaining data under section 55 of the 1998 Act and defences for journalistic activity. The provisions were never commenced. They are no longer needed because the offence of unlawfully obtaining data, defences and penalties are now set out in clauses 162 and 176 of this Bill.
- 795 Paragraph 23 omits Part 4 of the Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014, which sets rules for data processing by competent authorities based on the requirements of the 1998 Act. This Part is now redundant.
- 796 Paragraph 24 amends the Small Business, Enterprise and Employment Act 2015 by substituting references to the 1998 Act with references to the GDPR.
- 797 Paragraph 25 omits sections 108 to 110 of the Digital Economy Act which is concerned with charges payable to the Information Commissioner. These provisions have been superseded by clause 132 of this Bill.
- 798 Paragraph 26 provides that provisions added to secondary legislation by this Schedule can be amended by powers under the legislation they amended.

Commencement

799 The following provisions of the Bill will come into force on Royal Assent: Clauses 1 and 2 (preliminary), 169 (regulations under this Act), 183 to 185 (definitions), 188 and 189 (application to the Crown and Parliament), 191 to 194 (final provisions) and all powers to make secondary legislation. The other provisions of the Bill will be brought into force by regulations made by the Secretary of State. The GDPR comes into effect on 25 May 2018 and Member States are required to adopt laws giving effect to the LED by 6 May 2018.

Financial implications of the Bill

800 The financial costs and benefits of the Bill have been set out in accompanying impact assessments.

Parliamentary approval for financial costs or for charges imposed

801 This section will be completed when the Bill transfers to the House of Commons.

Compatibility with the European Convention on Human Rights

802 Lord Ashton of Hyde has made the following statement under section 19(1)(a) of the Human Rights Act 1998:

“In my view the provisions of the Data Protection Bill are compatible with the Convention rights.”

Article 6: Right to a fair trial

803 The defences to criminal offences in clauses 139, 160 to 163 and 171 are intended to place a legal burden on a defendant through the use of the term “prove”. The 1998 Act used both the terms “prove” and “show” in sections 47(3) and 55(2) respectively. Clause 176(3)-(6) makes an exception to section 127 of the Magistrates’ Court Act 1990 for an offence brought under clause 163 (alteration etc of personal data to prevent disclosure) so that the usual six month limitation period from the date of the offence runs instead from the date the prosecuting authority first knew of the possible offence, but for no longer than three years after the offence was committed.

804 The imposition of a legal burden on a defendant may interfere with their rights under Article 6 of the ECHR. The modification to standard limitation periods for criminal offences may also interfere with Article 6 rights.

805 Any interference with the Article 6(2) right must be according to law. The Government consider that the extent and nature of the factual matters the defendant is required to prove are not unduly onerous, and are likely to relate to matters which are more readily provable by the defendant than the prosecution. On balance the Government believe that the burden to prove the defence is justified having regard to the seriousness of the offence and to give effective enforcement support to the aims of a framework that regulates the processing of personal data. None of the offences will carry custodial penalties.

806 The modification to standard limitation periods is a practical step in light of the fact that such offences may not come to light until sometime after they have been committed. Such a modification is not unprecedented - see e.g. section 6 of the Road Traffic Offenders Act 1988. The three year long-stop provides a safeguard against the prospect of such a prosecution being brought within an indeterminate period. In the Government's view, any interference is proportionate.

Article 8: Right to respect for private and family life

807 The Bill includes a number of exemptions from the rights given to data subjects in the GDPR and obligations imposed on controllers in relation to personal data. These rights include the right of access to data (Article 15), the right of erasure (Article 17) and the right to receive certain information from the controller (Articles 13 and 14). Exemptions may also permit disclosure of personal data for a purpose other than the purpose for which the data was originally collected.

808 Restricting certain rights of data subjects and obligations of controllers could result in interference with Article 8 rights of individuals. The Government consider that the restrictions being made under the Bill meet the balancing test in Article 8(2) and therefore do not constitute an unlawful interference with Article 8 as they are proportionate in pursuit of a legitimate aim i.e. that in each case they are in the interests of public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others; and they are no more than are necessary and proportionate in a democratic society. The exemptions only apply to the extent of any prejudice to those interests and make the specific provisions and contain safeguards as required.

809 Article 9(1) of the GDPR prohibits the processing of special categories of data. These are: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. However, Article 9(2) permits the processing of this data in certain circumstances and subject to safeguards. Clause 9 gives effect to Schedule 1, which provides for derogations from the ban on processing of special categories of personal data where Member State law permits such processing for certain purposes. Schedule 1 sets out the general safeguards that are required to be applied by data controllers when processing under most of these conditions, which are in addition to the safeguards that may already be incorporated in a particular condition.

810 The Government consider that these potential interferences with Article 8 rights are justified as they are in accordance with the law, meet the test of necessity and proportionality and fall within one of the categories in Article 8(2) such as the protection of health.

811 Clause 17 exercises a derogation under Article 49(4) GDPR by enabling the Secretary of State to specify in regulations circumstances in which data transfer may or may not be taken to be necessary for important reasons of public interest, for the purpose of relying on Article 49(1)(d) GDPR to transfer personal data to a third country or international organisation. In exercising the power in the Bill to specify such circumstances, the Secretary of State could provide further grounds for transfers of personal data to third countries and international organisations. Such transfers could result in interferences with Article 8 rights of data subject.

812 Article 49(1)(d) GDPR resembles an existing provision in paragraph 4(1) of Schedule 4 to the 1998 Act. Paragraph 4(1) enables overseas transfers of personal data for reasons of substantial public interest, for example to help combat money laundering. Paragraph 4(2) of Schedule 4 gives the Secretary of State a similar power to that in clause 17, but the paragraph 4(2) power has not been exercised.

- 813 Any regulations made under clause 17 will, in accordance with that clause, be subject to parliamentary scrutiny (through the negative procedure) and to scrutiny by the courts, for example on grounds of irrationality or incompatibility with ECHR. The Government consider that these safeguards will ensure that any resulting interference with Article 8 rights is proportionate.
- 814 The approach adopted in the Bill to national security exemptions, mirrors the approach to national security in the 1998 Act. Clauses 24, 41(4), 42(4), 45(3), 65(7) and 110 provide for national security exemptions. Exempting from data protection standards in the relevant regimes on the grounds of national security necessarily interferes with Article 8 rights, as in such circumstances data controllers will be seeking to restrict the rights which data subjects would otherwise benefit from.
- 815 The approach in the Bill to national security exemptions will not change the existing position in the 1998 Act, which already provide a broad exemption from data standards. As a result, in the Government's view, the Bill itself will not be creating any greater interference with rights. Furthermore, the exemptions do not impact on the existing foreseeability position, with restrictions of data protection rights under the Bill no less foreseeable than under the 1998 Act.
- 816 In addition, the approach taken to exemptions in the Bill is consistent with Convention 108, Article 9 of which permits member states to restrict specified data rights and principles for the purposes of safeguarding national security. As a result the Government consider the national security exemptions provided for in the Bill are envisioned by the Convention and consistent with the ECHR. Any interference with Article 8 rights resulting from any restrictions on data rights is also clearly in pursuit of a legitimate aim, namely the safeguarding of national security.

Article 10: Freedom of expression

- 817 Article 85 of the GDPR requires Member States to provide exemptions or derogations from certain rights and obligations in the context of processing personal data for journalistic purposes or the purpose of academic, artistic or literary expression, if such exemptions or derogations are necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information. Part 4 of Schedule 2 exempts the data protection principles, many of the data subject rights and other obligations imposed on a data controller to the extent necessary to allow for publication of such material. Article 10 is engaged as there is an inherent tension between data protection, and the right to freedom of expression.
- 818 The limits imposed on the ability to rely on the exemption in paragraph 24 of Part 4 of Schedule 2 mean that the exemption from the privacy rights is only activated when necessary for publication and that publication is reasonably considered to be in the public interest. The Government's view is that this balances the right to privacy and the right to freedom of expression.

Related documents

819 The Government has published online a number of related documents:

<http://www.gov.uk/Government/collections/data-protection-bill-2017>

820 The following documents are relevant to the Bill,

- [The GDPR](#);
- [The LED](#);
- The [draft modernised Convention 108](#);
- [Call for Views on the GDPR derogations](#), DCMS, 12 April 2017;
- [A New Data Protection Bill: Our Planned Reforms](#) – Statement of Intent, DCMS, 7 August 2017;
- [The exchange and protection of personal data: a future partnership paper](#), HM Government, August 2017;
- Bill Impact Assessment;
- Delegated Powers Memorandum;
- European Convention on Human Rights Memorandum;
- Applied GDPR regime - “Keeling Schedule”.

Annex A – Glossary

Affirmative procedure	Statutory instruments that are subject to the “affirmative procedure” must be approved by both the House of Commons and House of Lords to become law.
Article 29 working party	The group of expert persons who advise member states on data protection. The group was established under Article 29 of European Data Protection Directive (Directive 95/46/EC) and is made up of a representative from the data protection authority of each Member State, the European Data Protection Supervisor and the European Commission. The Commissioner is the UK’s representative on the working party.
Convention 108	Council of Europe Convention for the protection of Individuals with regard to Automatic Processing of Personal Data.
Data controller	A “data controller” is responsible for complying with data protection law. They are defined in Article 4 of the GDPR as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data processor	A ‘data processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
DPIA	Data protection impact assessment
DPO	Data Protection Officer
ECHR	European Convention on Human Rights
EU	European Union
EEA	European Economic Area
GDPR	General Data Protection Regulation
LED	Law Enforcement Directive
ICO	Information Commissioner’s Office
Negative procedure	Statutory instruments that are subject to the “negative procedure” automatically become law unless there is an objection from the House of Commons or House of Lords.
Personal data	“Personal data” is defined in Article 4 of the GDPR as 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 data	“Processing” includes obtaining, recording, holding, using, disclosing or erasing data.
TFEU	Treaty on the Functioning of the European Union
The 1998 Act	Data Protection Act 1998
The 2014 Regulations	Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014 (SI 2014/3141)
The 2000 Act	Freedom of Information Act 2000
The 2016 Act	Investigatory Powers Act 2016
The Commissioner	The Information Commissioner

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

Annex B – LED Transposition Table

Article	Recital(s)	Copy out (yes/no)	If no – reason for elaboration or non-transposition	Corresponding clause
1	1 to 11	No	This article sets out the subject matter and overall objective of the LED and affords Member States scope to establish higher safeguards for the protection of data subjects. It does not impose additional obligations on Member States; as such, the article does not require separate implementation. However, a definition of law enforcement purposes is needed to reflect Article 2(1) (read with Article 1(1)).	27 and 29
2	11, 14, 17, 18, 20, 19, 33, 34	In part	The limitation on the scope of the LED in Article 2(1) and (2) is reflected in clause 26(1) and (2). Article 2(3)(a) has not been transposed as the provisions in Part 3 of the Bill apply to the domestic processing of data for law enforcement purposes as well as to the cross-border transfer of personal data; the former falls outside the scope of EU law. It is not necessary to transpose Article 2(3)(b) as Union institutions, bodies, offices and agencies do not constitute competent authorities for the purposes of Part 3 of the Bill.	27
3	12, 13, 18, 23 & 24	In part	<p>The definition of “personal data” in clause 2(2) substantially copies out that in Article 3(1) but refers to a “living person” rather than a “natural person” for consistency with the approach taken in the GDPR (see recital 27). Linked to this, clause 2(5) includes a definition of “data subject” (the definition of “personal data” in Article 3(1) adopts the term “data subject” but (unlike the 1998 Act) leaves it undefined).</p> <p>For legal clarity Schedule 7 contains a list of the primary competent authorities to whom Part 3 of the Bill applies rather than adopt the definition in Article 3(7). Other competent authorities are caught by clause 28(1)(b).</p> <p>The definitions of “processor” and “recipient” refer to “any person”, a term which covers “a natural or legal person, public authority, agency or [an] other body” (see Schedule 1 to the Interpretation Act 1978).</p> <p>It is not necessary to transpose the latter part of the definition of “recipient” in Article 3(10) as UK public authorities would be bound by the rules applicable to the processing in question.</p> <p>Part 3 of the Bill does not include a definition of “supervisory authority” (Article 3(15)); the Information Commissioner, as provided for in Part 5, is the supervisory authority for the LED.</p>	2(2), (4), (5) and (7), 28, 29, 30, 31, and 184 and Schedule 7
4	26 to 30	In part	Clause 32 provides an overview of the six data protection	32, 33(1), 34, 35, 36(1), 37, 38, 39

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

Article	Recital(s)	Copy out (yes/no)	If no – reason for elaboration or non-transposition	Corresponding clause
			<p>principles set out in Article 4(1) and amplified in Articles 5 to 10</p> <p>In transposing Article 4(4), clause 31(3) applies the general duty of the controller to the whole of Chapter 2 of Part 3 as, in demonstrating compliance with the data protection principles, a controller will need to comply with the associated Articles.</p> <p>In transposing Article 4(1)(e) the reference to personal data being kept “in a form which permits identification of data subjects” has not been transposed given that by definition (see Article 3(1)) personal data must permit the identification, either directly or indirectly, of data subjects.</p>	and 40
5	26 and 41	In part	Article 5 affords Member States the option of providing for appropriate time limits for either the erasure of personal data or for a periodic review of the need for storage of personal data. In transposing this Article, the Government has opted for review rather than erasure.	37(2)
6	31	In part	For greater clarity, clause 36(3) in places adopts different language to that used in Article 6. In any event, the list of categories of data subject in this Article is an indicative rather than exhaustive one.	36
7	32	Yes	N/A	36(2), (4) and (5)
8	33 to 35	In part	Part 3 of the Bill does not transpose Article 8(2) on the basis that is a matter for the relevant statute or case law regulating processing to specify the objectives of processing, the personal data to be processed and the purpose of the processing.	33
9	36	No	<p>Clause 33(4) gives effect to the provision in the first sentence of Article 9(1). As Part 3 only applies in relation to processing for law enforcement purposes, the effect of the overall scheme in the Bill would be for a competent authority to process data for any other lawful purpose under the provisions of the GDPR or applied GDPR as appropriate.</p> <p>As the ambit of Articles 9(3) and (4) is unclear, clause 78 is considered necessary to provide clarity and give effect to these provisions by providing the controller must consider if the personal data would be subject to any restrictions by virtue of enactment or rule of law, and where this is the case, the controller must inform the EU and non EU recipient, that the data is made available with the same restrictions.</p>	34(2)-(4) and 78
10	37	Yes	N/A	33(3)-(5) and Schedule 8
11	38 and 51	Yes	N/A	45 and 46
12	39 and 40	In part	Article 12(1) requires, “as a general rule”, a controller to provide information to a data subject in the same form as the request.	42, 43, 44, 50, 51

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

Article	Recital(s)	Copy out (yes/no)	If no – reason for elaboration or non-transposition	Corresponding clause
			<p>Rather than adopt the qualification in Article 12(1), clause 49(3) sets aside the requirement where it would be impractical to provide the information in the same form as the request, for example, where the request was made orally.</p> <p>Clause 50(4)(b) amplifies Article 12(5) to make it clear that, in a case where there is doubt about the identity of a person making a request in accordance with Article 14 or 16, the controller is not required to act on the request until the person's identity has been confirmed.</p> <p>Article 12(4) enables a controller to charge a reasonable fee where a request from a data subject is manifestly unfounded or excessive; clause 51(4) and (5) augments this provision by providing for a power, by regulations, to prescribe a maximum fee.</p>	and 52
13	42	In part	Article 13(4) enables Member States to adopt measures in order to determine categories of processing which may fall under any of the points in Article 13(3); the Government has not given effect to this derogation.	42 and 43
14	43	Yes	N/A	42(1) and (2)
15	44 to 46	In Part	Article 15(2) enables Member States to adopt measures in order to determine categories of processing which may fall under any of the points in Article 15(1); the Government has not given effect to this derogation.	43(4)
16	47	In part	<p>Article 16(1) confers a right to obtain rectification and Article 16(2) confers a right to obtain erasure; although there is no express mention of a right to obtain a restriction on processing such a right is implied by Articles 13(1)(e), 14(e) and 16(4). Clause 45(2) therefore requires a controller to respond to a request of this kind.</p> <p>The additional words in brackets in clause 44(4) clarify that the duty to erase in Article 16(2) does not depend on any request being made by the data subject, in contrast to the duty to rectify in Article 16(1).</p> <p>Article 16(5) requires a controller to communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate personal data originate. The addition of the words "if any" in clause 46(7) recognises that there could be cases where there is no competent authority from which the inaccurate personal data originates.</p>	44 to 46
17	48	Yes	N/A	49
18	49	Yes	N/A	41(3) and (4)
19	53	In part	The reference to risks "of varying likelihood and severity" in Article 19(1) has not been reproduced as it is sufficient to state that all risks are taken into account.	54
20	52, 53	In part	The reference to risks "of varying likelihood and severity" in Article 20(1) has not been reproduced as it is sufficient to state that all risks are taken into account. The references to	55

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

Article	Recital(s)	Copy out (yes/no)	If no – reason for elaboration or non-transposition	Corresponding clause
			“pseudonymisation” and “data minimisation” have not been reproduced as these are intended only as examples and, as such, more appropriately referred to in guidance. It is not considered necessary to transpose the closing words of Article 20(1) as they do not add anything of substance to the duty placed on controllers.	
21	54	In part	It is not considered necessary to transpose the wording “in particular as regards the exercise of the rights of the data subject and their respective duties to provide the information referred to in Article 13” in Article 21(1) as it simply elaborates rather than alters the nature of the duty on joint controllers. Article 21(2) confers a discretion on Member States, this has been exercised by a provision (in clause 56(3)) enabling a data subject to exercise his or her rights against any joint controller.	56
22	55	In part	The reference, in Article 22(4), to a contract between a processor and controller being in writing is considered sufficient without the added reference to “including in an electronic form”.	57
23	50	Yes	N/A	58
24	56	In part	It is not considered necessary to transpose the requirement, in Article 24(3), that the records of processing activity must be in writing as this is implicit. The requirement in Article 24(3) for the record to be in electronic form has not been provided for.	59
25	57	In part	Clause 60(1) makes it clear that the duty to keep logs falls on the processor, and not the controller, where a processor is processing personal data on behalf of the controller.	60
26	59	Yes	N/A	61
27	58	In part	It is not considered necessary to transpose the wording “in particular, using new technologies” in Article 27(1) as it simply elaborates rather than alters the nature of the duty on controllers.	62
28	59	In part	Article 28(1) provides the controller <u>or</u> processor must consult the Information Commissioner, in certain cases, prior to processing; clause 63(1) places this duty only on the controller only. Any advice provided by the Information Commissioner would, however, be provided to the controller and any processor. This approach better reflects the intended responsibilities of controllers and processors. It is not considered necessary to reproduce the words from “in particular” in Article 28(4).	63
29	53, 56 and 60	In part	The reference to risks “of varying likelihood and severity” in Article 29(1) has not been reproduced as it is sufficient to state that all risks are taken into account. It is not considered necessary to transpose the wording “in particular as regards the processing of special categories of personal data referred to in Article 10” in Article 29(1) as it simply elaborates rather than alters the nature of the duty on controllers and processors. Clause 64(2) provides for a more streamlined list of the outcomes to be secured by the adoption of appropriate security measures compared with that in Article 29(2).	64
30	61	Yes	N/A	65
31	62	Yes	N/A	66

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

Article	Recital(s)	Copy out (yes/no)	If no – reason for elaboration or non-transposition	Corresponding clause
32	63	In part	It is unnecessary to refer to “independent” judicial authorities as in Article 32(1) as all UK judicial authorities are considered to be independent.	67
33	63	In part	Clause 68(3) to (5) makes provision akin to that set out in Article 38(3) to (6) of the GDPR, which is not mirrored in the LED, to ensure consistency between the two regimes insofar as it relates to data protection officers.	68
34	63	In part	Clause 69(3) makes provision akin to that in Article 39(2) of the GDPR, which is not mirrored in the LED, to ensure consistency between the two regimes insofar as it relates to data protection officers performing their tasks.	69
35	64 and 65	In part	It is not considered necessary to transpose the reference to personal data “undergoing processing or are intended for processing” in Article 35(1). Article 35(1)(e) refers to the seriousness of the criminal offence, clause 76(3)(a) generalises the wording as the law enforcement purposes are not confined to activities relating to criminal offences. Article 35(3) is a purpose provision which does not require specific transposition.	71 and 76
36	66	In part	Article 36(2) to (6) and (8) do not require transposition as they place obligations on the European Commission rather than the Member State. Article 36(7) provides that the suspension or repeal of an adequacy decision in respect of a third country does not affect the ability to transfer data to that third country in reliance on Articles 37 or 38; clause 71(3) achieves this without the need for more in clause 72.	72
37	67 to 71	In part	Clause 73(3)(c)(iv) clarifies that the duty, in Article 37(3), to document the personal data transferred should be read as a duty to provide a description of the personal data transferred, rather than the data itself.	73
38	72	In part	It is not considered necessary to transpose the words “where the law of the Member State transferring the personal data so provides” in Article 38(1)(b) as to do so may be taken to narrow the class of “legitimate interests”. Clause 74(4) adopts the definition of a “legal purpose” in paragraph 5 of Schedule 4 to the 1998 Act. .	74
39	73	In part	It is not considered necessary to refer to both an “individual” and “specific” case on the basis that “specific” by itself conveys the intention.	75
40	74 and 83	In part	This Article replicates the GDPR Article 50 which is considered and provided for in Part 5 of the Bill.	116
41	76	No	Article 41 requires Member States to provide for one or more supervisory authorities responsible for monitoring the application of the LED. A supervisory authority established under the GDPR	112

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

Article	Recital(s)	Copy out (yes/no)	If no – reason for elaboration or non-transposition	Corresponding clause
			may also discharge the functions of a supervisory authority under the LED. The Bill provides for the Information Commissioner to be the supervisory authority for the purposes of the GDPR and LED. As the Information Commissioner is the sole UK supervisory authority, nothing is required in respect of Article 41(4).	
42	75, 78	No	No express legislative provisions are considered to be required in relation to Article 42(1) to (3). The independence of the Information Commissioner derives from the totality of the legislative framework under which she operates, including the absence of any powers for a Minister of the Crown to direct the Commissioner (subject to the limited exception in clause 124). Provision in respect of conflicts of interest (Article 42(3)) would be included in Commissioner's terms of appointment. Paragraph 5 of Schedule 12 makes provision for the appointment of staff of the Information Commissioner (Article 42(4) and (5)) and paragraphs 9 to 11 of Schedule 12 makes provision for the funding of the Information Commissioner the treatment of fee income and accounts (Article 42(6)).	Schedule 12
43	79	No	Article 43(1) confers discretion on Member States, subject to specified parameters, to determine the person responsible for appointing each member of the supervisory authority; paragraph 2 of Schedule 12 provides for the Information Commissioner to be appointed by Her Majesty (on the recommendation of the Secretary of State for Digital, Culture, Media and Sport). Article 43(2) does not require legislative provision; the appropriate qualifications, experience and skills would be set out in the role profile when recruiting an Information Commissioner and candidates will be judged against the role profile. Article 43(3) does not require legislative provision; the duties of the Information Commissioner automatically terminate once an individual no longer holds that office. Paragraph 3 of Schedule 12 provides for an exhaustive list of grounds for the removal of the Information Commissioner.	Schedule 12, paragraph 3
44	77	No	Clause 112 provides for the continuance of the office of Information Commissioner (Article 44(1)(a)). Article 44(1)(b) does not require legislative provision; the appropriate qualifications, experience and skills would be set out in the role profile when recruiting an Information Commissioner and candidates will be judged against the role profile. Paragraph 2 of Schedule 12 provides for the appointment of the Information Commissioner; the procedure for making an appointment is set down in a Governance Code. Paragraph 2(3) and (4) of Schedule 12 provides for the Commissioner to be appointed for a single term of up to seven years (Article 44(1)(d) and (e)). Provision in respect of conflicts of interest and duty of professional secrecy (Article 44(1)(f) and (2)) would be included in the terms and conditions of appointment of the Commissioner and members of staff. In addition, clause 127 provides for an offence of unlawful disclosure by Information Commissioner staff.	127 and Schedule 12
45	80	No	It is not considered necessary to transpose Article 45(1) on the basis that the measures in Part 5 of the Bill relating to the functions and powers of the Information Commissioner satisfy the requirements of this provision.	115

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

Article	Recital(s)	Copy out (yes/no)	If no – reason for elaboration or non-transposition	Corresponding clause
46	80 and 81	In part	It is not considered necessary to transpose Article 46(3). As a corporation sole the Information Commissioner will only have the powers conferred on her by statute. So, in the absence of an express power to charge fees, she will not be able to do so. Clause 129 enables the Commissioner to charge fees to persons other than data subjects and data protection officers.	114, 118 and 130, Schedule 13 and Part 1 of Schedule 14
47	82	No	Article 47 requires Member States to provide for the national supervisory authority to have effective investigative, corrective, advisory and enforcement powers, but otherwise leaves it to Member States as to the precise form of such powers.	Part 5
48	82 and 61	Yes	N/A	79
49	N/A	In part	Clause 134 provides for the Information Commission to make an annual report to Parliament; it is not considered necessary to give examples of the matters that may be addressed in the report (as in Article 49). The duty to publish the annual report satisfies the requirement to make it available to the public and others.	134
50	83	In Part	Article 50 provides for how the EEA supervisory authorities shall cooperate. Article 50 (8) has not been transposed because of the role of it gives to the European Commission in specifying what and how the supervisory authorities cooperate.	Part 1 of Schedule 14
51	84	No	This Article adds to the functions of the European Data Protection Board established by the GDPR. As an EU body, domestic legislation is not required to give effect to this Article.	N/A
52	85 and 81	Yes	N/A	156
53	86	No	This Article requires Member States to provide for a judicial remedy against decisions of the supervisory authority. Such a remedy needs to reflect the judicial systems of each Member State.	154, 155 and 157
54	87	No	This Article requires Member States to provide for a judicial remedy against actions of a controller or processor. Such a remedy needs to reflect the judicial systems of each Member State.	158
55	87	Yes	Article 55 allows for data subject to mandate a not-for-profit body to lodge a complaint on his or her behalf. In this context the article has been interpreted so as to allow for charities and not for profit bodies with a data protection mandate and public interest objectives to take forward complaints.	173
56	88	Yes	Article 56 provides for compensation to be made available if contravention of the Directive leads to damage to a data subject. The article sets out the liability of each of the controller and the processor and when the right to compensation does not apply.	160
57	89	No	Article 57 requires Member States to provide for effective, proportionate and dissuasive penalties for infringements of the provisions of the LED, but otherwise leaves it to Member States to determine the appropriate penalties.	142 to 146, 148 to 152, 154 and 155
58	90, 91 and 92	No	This Article extends the remit of the committee established under Article 93 of the GDPR to assist the Commission. As an EU body, domestic legislation is not required to give effect to this Article.	N/A
59	98	No	Part 4 of the Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014 gave effect to Framework Decision 2008/977/JHS	Paragraph 23 of Schedule 18

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

Article	Recital(s)	Copy out (yes/no)	If no – reason for elaboration or non-transposition	Corresponding clause
			– Part 4 of the Regulations is repealed by Schedule 18.	
60	97	No	Article 60 specifies that EU legal provisions relating to the protection of personal data in judicial or police cooperation and criminal matters which regulate the processing between member states (or designated authorities) that entered into force on or before 6 May 2016, will remain unaffected. Domestic provision is not required to give effect to this Article.	N/A
61	94 and 95	No	Article 61 provides for the lawfulness of international agreements made prior to 06 May 2016 for cooperation in criminal matters. Domestic provision is not required to give effect to this Article.	N/A
62		No	Article 62 (GDPR Article 97) places a duty of the European Commission to review the Directive every 4 years and produce a report on the effectiveness of the Directive. Domestic provision is not required to give effect to this Article.	N/A
63	93, 96, 99, 100, 101, 102, 103, 104 and 105	No	This Article requires Member States to transpose the LED into domestic law by 6 May 2018. The provisions of the Bill giving effect to the LED will be brought into force by commencement regulations made under clause 191. Clause 192 enables regulations to make transitional provision as provided for in Article 63(2) and (3)	191 and 192
64	96	No	Relates to the coming into Force of the Directive. Domestic provision is not required to give effect to this Article.	N/A
65		No	Article 65 provides the addresses for the European Parliament and European Council. Domestic provision is not required to give effect to this Article.	N/A

Annex C – Convention 108

This table maps across the Articles of the draft modernised Convention 108 (available [here](#)) to the provisions of Part 4 of the Bill (together with the provisions in Parts 5 to 7 insofar as they relate to Part 4).

Article	Corresponding clause/Schedule or, where applicable, reason why express provision is not required
1	This Article sets out the object and purpose of Convention 108. It does not impose additional obligations on Parties to the Convention; as such, the Article does not require separate implementation.
2	Clauses 2(2) and (4), 81 and 82
3	Clause 80 limits the scope of Part 4 to processing by an intelligence service. Other data processing is governed by the GDPR, applied GDPR and law enforcement schemes.
4	The provisions in Part 4 of the Bill and elsewhere give legislative effect to the provisions of the Convention in relation to processing by an intelligence service. It is not considered necessary to make further legislative provision to give effect to paragraphs 2 and 3 of this Article.
5	Clauses 84 to 88 and Schedule 9
6	Clause 84 and Schedule 10
7	Clauses 89, 105 and 106
7bis	Clause 91
8	Clauses 92 to 98 and paragraph 7 of Schedule 14
8bis	Clauses 100 to 104
9	Clauses 108 to 111 and Schedule 11
10	Part 6
11	This Article enables a Party to the Convention to grant data subjects extended protection than that provided for in the Convention. The GDPR, applied GDPR and LED regimes provide for such extended protection where personal data is being processed by controllers other than the intelligence services.
12	Clause 107
12bis	Clause 114(1)(b) and Schedule 13
13	Clauses 114(1)(b) and 118 and paragraphs 6 and 10 of Schedule 14
14	Paragraph 8 of Schedule 14
15	Paragraph 9 of Schedule 14

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

16	Paragraph 6 of Schedule 14 imposes a duty on the Commission to co-operate with foreign designated authorities. As a creature of statute, the Commission cannot act in a way incompatible with its powers.
17	As a creature of statute, the Commission may only charge for services where there is express provision for such charges.
18 to 20	These Articles relate to the establishment and operation of a Convention Committee; as such, the Articles do not require separate UK implementation.
21	This Article deals with the procedure for amending the Convention; as such, the Article does not require separate UK implementation.
22	This Article provides for the entry into force of the Convention. The provisions in Part 4 of the Bill will be commenced by regulations – see clause 191.
23 to 27	These Articles make further procedural provision about the implementation of the Convention; they do not require separate UK implementation.

Annex D – Territorial extent and application in the United Kingdom

In the view of the Government of the United Kingdom, the provisions in clause 177 (recordable offences) of the Bill relate exclusively to England and Wales and it would be within the legislative competence of the Scottish Parliament and/or Northern Ireland Assembly to make corresponding provision. The provisions in clause 178 (guidance about PACE codes of conduct) also relate exclusively to England and Wales but, in the view of the Government of the United Kingdom, it would not be within the legislative competence of the Scottish Parliament and/or Northern Ireland Assembly to make corresponding provision. Clauses 175 and 176 and Schedule 18 apply in part to England and Wales (and wholly or partly to Scotland and Northern Ireland), clause 187 applies to Scotland only and Schedule 12 applies to England and Wales and Northern Ireland and, in part, to Scotland. All the other provisions of the Bill form part of the law of the UK.

Provision	Extends to E & W and applies to England?	Extends to E & W and applies to Wales?	Extends and applies to Scotland?	Extends and applies to Northern Ireland?	Would corresponding provision be within the competence of the National Assembly for Wales?	Would corresponding provision be within the competence of the Scottish Parliament?	Would corresponding provision be within the competence of the Northern Ireland Assembly?	Legislative Consent Motion needed?
Part 1 Preliminary Clauses 1-2	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Part 2 - General Processing Clauses 3-26	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Part 3 – Law Enforcement Processing Clauses 27-79	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Part 4 – Intelligence Services Processing Clauses 80-111	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Part 5 – The Information Commissioner Clauses 112 136	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Part 6 – Enforcement								

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

Provision	Extends to E & W and applies to England?	Extends to E & W and applies to Wales?	Extends and applies to Scotland?	Extends and applies to Northern Ireland?	Would corresponding provision be within the competence of the National Assembly for Wales?	Would corresponding provision be within the competence of the Scottish Parliament?	Would corresponding provision be within the competence of the Northern Ireland Assembly?	Legislative Consent Motion needed?
Clauses 137-168	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Part 7 – Supplementary and Final Provision Clauses 169-174	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Clauses 175-176	In part	In part	In part	In part	N/A	N/A	N/A	No
Clause 177	Yes	Yes	No	No	No	Yes	Yes	No
Clause 178	Yes	Yes	No	No	No	No	No	No
Clauses 179-186	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Clause 187	No	No	Yes	No	N/A	N/A	N/A	No
Clauses 188-190	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Schedules 1-11	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Schedule 12	Yes	Yes	In part	Yes	N/A	N/A	N/A	No
Schedules 13-17	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Schedule 18	In part	In part	Yes	In part	N/A	N/A	N/A	No

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66)

Minor or consequential effects⁹

There are no provisions which extend to the whole of the UK but where the effect in Scotland and Northern Ireland is only minor or consequential.

Subject matter and legislative competence of devolved legislatures

Clause 178 amends the National Police Records (Recordable Offences) Regulations 2000 to have effect as if offences under the Bill were added to the list of specified offences recorded in national police records. Those regulations, and therefore this clause, extend and apply to England and Wales only.

Policing is not devolved to the Welsh Assembly under the Government of Wales Act 2006 (Schedule 7). In relation to Scotland, the governance and administration of Police Scotland is not generally reserved to the UK Government under the Scotland Act 1998 (Schedule 5). In relation to Northern Ireland, the governance and administration of the Police Service of Northern Ireland is not generally an excepted or a reserved matter under the Northern Ireland Act 1998 (Schedules 2 and 3). It would be within the legislative competence of the Scottish Parliament and Northern Ireland Assembly to make provision corresponding to that in clause 178 in relation to the recording in police records of offences provided for in the Bill.

Clause 179 places a duty on the Commissioner to produce and publish guidance about how the Commissioner proposes to perform the duty, under section 67(9) of the Police and Criminal Evidence Act 1984 (“PACE”), to have regard to codes of practice under that Act when investigating offences and charging offenders in respect of offences under the Bill. The clause extends to the whole of the UK, reflecting the jurisdiction of the Commissioner, but the PACE codes of practice apply to England and Wales only, accordingly guidance produced under this clause will only impact in that jurisdiction. As data protection, including the functions of the Commissioner, is a reserved matter it would not be within the legislative competence of the Scottish Parliament or Northern Ireland Assembly to make provision corresponding to that in clause 179 in relation to the conferral of functions on the Commissioner akin to those conferred by clause 179.

⁹ References in this Annex to an effect of a provision being minor or consequential are to its being minor or consequential for the purposes of Standing Order No. 83J of the Standing Orders of the House of Commons relating to Public Business.

DATA PROTECTION BILL [HL]

EXPLANATORY NOTES

These Explanatory Notes relate to the Data Protection Bill [HL] as introduced in the House of Lords on 13 September 2017 (HL Bill 66).

Ordered by the House of Lords to be printed, 13 September 2017

© Parliamentary copyright 2017

This publication may be reproduced under the terms of the Open Parliament Licence which is published at www.parliament.uk/site-information/copyright

PUBLISHED BY AUTHORITY OF THE HOUSE OF LORDS