EXPLANATORY NOTES

Data Protection Act 2018

Chapter 12

tso
part of Williams Lea Tag

Published by TSO (The Stationery Office), part of Williams Lea Tag, and available from:
Online
www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries: 0333 202 5070
Fax orders: 0333 202 5080
E-mail: customer.services@tso.co.uk
Textphone: 0333 202 5077

TSO@Blackwell and other Accredited Agents

ISBN 978-0-10-560089-3

9 780105 600893

DATA PROTECTION ACT 2018

EXPLANATORY NOTES

What these notes do

These Explanatory Notes relate to the Data Protection Act 2018 (c. 12) which received Royal Assent on 23 May 2018.

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

Table of Contents

Overview of the Act

1 The Data Protection Act 2018 ("the Act") 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 Act also helps prepare the UK for a future outside the EU.

2 The four main matters provided for in the Act are general data processing, law enforcement data processing, data 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 previous law on data protection was found in the Data Protection Act 1998 ("the 1998 Act"), which regulated the processing of personal data. The 1998 Act protected the rights of individuals to whom the data related.

4 The new Act replaces the 1998 Act to provide a comprehensive legal framework for data protection in the UK, in accordance with the General Data Protection Regulation ((EU) 2016/679) ("GDPR"). It updates the rights provided for in the 1998 Act to make them easier to exercise and to ensure they continue to be relevant with the advent of more advanced data processing methods.

5 The Act implements commitments to update data protection laws made in the 2017 Conservative Manifesto and modernises data protection laws in the UK to meet the needs of our increasingly digital economy and society.

6 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 became the 51st Party to the Convention. The Committee of Ministers of the Council of Europe adopted a modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data ("modernised Convention 108") on 18 May 2018. The modernised treaty will be opened for signature on 25 June 2018. The Act has been designed so as to be consistent with the modernised Convention 108.

7 The UK's data protection laws, therefore, need to interlock with international data protection arrangements. In addition to Convention 108, the 1998 Act implemented the European Data Protection Directive (Directive 95/46/EC) ("the 1995 Directive"). On 25 May 2018 the Directive will be replaced when the GDPR begins to apply.

8 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.

9 On 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.

10 The Act is structured in seven parts. Part 1 contains preliminary matters. Part 2 must be read alongside the GDPR and sets out certain derogations from the GDPR. This Part also 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. Part 3 contains provision for law enforcement data processing and Part 4 provides likewise for data processing by the intelligence services. The remaining parts are concerned with the Information Commissioner (the "Commissioner"), enforcement and offences, and supplementary provision.

General Data Protection Regulation

11 To fully understand the Government's legislative intent as found in this Act, it may be necessary to have some wider background understanding of the GDPR.

Definitions and scope

12 The GDPR changes some of the definitions that set the scope of data protection law. Like the 1998 Act before it, 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. Personal data that has been pseudonymised, for example key-coded data, can fall within the scope of the GDPR if it is still possible to attribute the pseudonym to a particular individual.

13 The 1998 Act provided additional safeguards for "sensitive personal data" which included 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

14 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.

	The former Data Protection Act 1998 principles	**The new General Data Protection Regulation principles**
Lawfulness	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.
Purpose	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.
Data minimisation	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.
Accuracy	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.
Storage	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.
Access	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.
Security	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.
Overseas transfer	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.
Accountability	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

15 Article 6 of the GDPR sets out the different legal bases under which personal data can be lawfully processed. A common way 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.

16 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).

17 Consent is not the only way to enable processing of personal data. As an alternative to consent, there may be a contractual or other legal obligation that allows data to be processed. Data may also 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.

18 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 when performing their public tasks. 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.

19 Where explicit consent is not obtained, there are additional limitations on when data can be lawfully processed for special categories of personal data and personal data relating to criminal convictions etc.

Individuals' rights

20 The rights that individuals had 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.

	Former Data Protection Act 1998 rights	**The new General Data Protection Regulation rights**
The right to be informed	The 1998 Act provided the right to 'fair processing information', typically given through a privacy notice. The information had to include: • 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.	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.
The right of access	The 1998 Act provided 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.	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.
The right to rectification	Where the personal data held about them was inaccurate, the individual concerned had a right to apply to the court for an order to rectify, block, erase or destroy the	Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. It must 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

	inaccurate information.	seek a judicial remedy.
The right to erasure	The 1998 Act did not provide the right to erasure, but an individual could apply to a court for an order for erasure of inaccurate personal data.	Individuals have a right to have personal data erased in specific circumstances: • 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.
The right to restrict processing	The 1998 Act allowed individuals to apply to a court for an order to block or suppress processing of personal data where it is inaccurate. When processing was restricted, it was permissible to store the personal data, but not further process it.	Where it is claimed that data is inaccurate individuals can require the controller to restrict processing until verification checks have been completed. Individuals may also require controllers to restrict processing where the controller no longer needs to (other than for legal claims).
The right to data portability	Not applicable	The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services where processing is based on consent or performance of a contract. 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. The personal data must be provided in a structured, commonly used and machine readable form. The information must be provided free of charge.
The right to object	The 1998 Act provided individuals with the right to object to the processing of personal data for direct marketing.	In addition to being able to object to direct marketing, individuals have the right to object to processing (including profiling) based on legitimate interests or the performance of a task in the public interest/exercise of official authority, and processing for purposes of scientific/historical research and statistics.
Rights in relation to automated decision making and profiling	The 1998 Act allowed an individual access to information about the reasoning behind any decisions taken by automated means. An individual could give written notice requiring that automated decisions are not made using their personal data. Individuals	The GDPR provides similar rights and additionally defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual.

	could ask for a decision taken by automated means to be reconsidered.	

General processing

21 Chapter 2 of Part 2 of the Act 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

22 The key terms used in the GDPR are largely consistent with the 1998 Act but the new Act 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 new Act ensures that the clarity in section 1(4) is preserved.

23 The term 'public authority' is not defined in the GDPR. For clarity and legal certainty the Act adopts the definitions in the Freedom of Information Act 2000 ("the 2000 Act") and the Freedom of Information (Scotland) Act 2002, subject to two qualifications. First, public authorities are only to be treated as public authorities for the purposes of the GDPR when they are carrying out a task in the public interest or in the exercise of official authority vested in it. Second, the Act specifically excludes parish councils, community councils and similar bodies from the definition because in the government's view these bodies are very small in terms of personnel, budget and the volume of personal data processed such that the additional safeguards that public authorities normally have to apply would be disproportionate in these instances.

Lawfulness of processing

24 The Act is drafted to ensure that existing data processing can continue, subject to the enhanced rights provided by the GDPR.

25 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 was silent on this matter but the Commissioner's guidance suggested that some form of parental consent would normally be required before collecting personal data from children under 12. The new Act allows a child aged 13 years or older to consent to his or her personal data being processed by providers of information society services.

26 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 explicit 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 Act replicates the former provisions in the 1998 Act that allowed the processing of this sort of data. The new

Act 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, while also making some new provision. The Act 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 (S.I. 2000/417).

27 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 (S.I. 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 Act provides the Secretary of State with the necessary power to manage unforeseeable situations of this sort.

28 The GDPR gives individuals the right to not be subject to a decision based solely on automated processing, including profiling, which have legal or other significant effects for him or her, unless that decision is necessary for contractual purposes, authorised by law and appropriate safeguards are in place, or based on consent. Automated processing is processing where there is no human intervention, for example, when data is collected about an individual's personal finances, which is then processed according to an algorithm to decide creditworthiness. In those cases in which automated decision making is allowed, the GDPR requires additional safeguards to be put in place to protect individuals from inaccurate processing. The Act substantively replicates the additional safeguards provided within section 12(2) of the 1998 Act and ensures they are consistent with relevant provisions of the GDPR itself.

Individuals' rights

29 There are some limited circumstances where it is appropriate to create exemptions to the usual rights that individuals have over their personal data. The Act ensures that exemptions in the 1998 Act continue to apply, as well as introducing a number of new restrictions.

30 The 1998 Act contained exemptions to disapply individual rights in relation to personal data held by regulatory bodies performing functions concerned with protecting the public from incompetence, malpractice, dishonesty or seriously improper conduct, or concerning health and safety; charities; or ensuring fair competition in business. For example, without appropriate exemptions a corrupt official might be able to find out how his or her corruption is being exposed. Similarly exemptions exist to ensure that the judiciary have a 'safe space' in which to conduct their work, where they are free to make such records in the course of reaching their judgment, without fear that such records (such as annotations, recorded discussions) may be investigated or challenged by parties to proceedings. The Act ensures that exemptions of this sort continue to be available.

31 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 provided for separately in the Act, 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 enabled Her Majesty's Revenue and Customs ("HMRC") to withhold certain personal data on a case by case basis from an individual customer who submitted a subject access request if providing that personal data would be

likely to prejudice specified crime and taxation purposes. It also meant that HMRC was not obliged to send a privacy notice to an individual when obtaining personal data from a third party if it would tip them off about an ongoing investigation into their tax affairs. The Act makes equivalent provision.

32 In the context of health, social work and education, there is sometimes information that is recorded about a person that is given on the condition that it is not disclosed to the person. If such information was disclosable the information would not be given. This could, for example, result in safeguarding concerns or limit a Court's ability to properly assess the best interests of the child in proceedings concerned with the care of children. Disclosure of personal data could also result in serious harm to the data subject or another individual. The 1998 Act and various orders made under powers in the Act provided exemptions to in respect of health, social work and education data. For example, the Data Protection (Subject Access Modification) (Health) Order 2000 (S.I. 2000/413) applied to personal data consisting of information as to the physical or mental health or condition of the data subject. The Act ensures that exemptions of this sort continue to apply.

33 The 1998 Act provided that personal data processed only for research, historical or statistical purposes could be exempted from subject access requests, subject to its being processed in compliance with certain conditions. The new Act exercises all of the derogations in Article 89(2) and (3) of the GDPR, and retains the relevant conditions, 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 Act 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.

34 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 Act therefore provides the Secretary of State with the power to make further exemptions in future.

Other general processing

35 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 Act contains provision to extend GDPR standards to data processing, other than processing falling within Part 3 (law enforcement processing) or Part 4 (intelligence services processing), to create a simple framework under which data controllers and processors can apply a single standard.

36 The Act achieves this by applying the Articles of the GDPR to general data outside the scope of Union law. For the applied GDPR, Schedule 6 modifies those Articles to make them relevant to a context where Union law does not apply (creating "the applied GDPR"). 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 are not relevant and are removed or amended.

Law enforcement processing

37 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 the GDPR, the European Parliament and Council adopted the Law Enforcement Directive (EU) 2016/680[1] "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" ("LED").

38 Unlike the GDPR, the LED is not directly applicable EU law; accordingly Part 3 of the Act (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.

39 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 incidental law enforcement functions, such as Her Majesty's Revenue and Customs, the Health and Safety Executive and the Office of the Information Commissioner.

40 While the LED only applies in relation to the cross-border processing of personal data for law enforcement purposes (see below), Part 3 of the Act also applies to the domestic law enforcement processing. This will ensure that there is a single domestic and trans-national regime for all law enforcement processing. The provisions of the GDPR, together with the derogations in Chapter 2 of Part 2 of the Act, will apply to the processing of personal data by law enforcement agencies for purposes other than law enforcement purposes, for example where the controller determines that the processing is for internal personnel management/ human resources purposes.

Intelligence services processing

41 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 or LED.

42 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. Part 4 of the new Act builds on the existing regime by seeking to adopt the standards of the modernised Convention 108 (which does apply to national security data processing) to ensure processing of personal data carried out by the

[1] 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

intelligence services will be in-line with 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.

43 As was the case previously under the 1998 Act, the regime in Part 4 of the Act provides for exemptions from certain provisions in the Act where necessary to safeguard national security. Also consistent with the approach in 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.

44 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.

45 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

46 The Act provides for the Commissioner to continue as the supervisory authority in the UK in relation to the protection of personal data (see sections 115(1) and 116(1)).

47 The powers of the Commissioner to investigate and sanction data protection breaches 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 originally enacted, the Commissioner could only serve enforcement notices and her powers to impose fines were only introduced under 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, and the Act, confer new powers on the Commissioner to impose a maximum fine of £17 million (€20 million) or 4 percent of turnover in the most serious cases. The GDPR and LED require fines to be effective, proportionate and dissuasive in each individual case. The Act ensures that the Commissioner's powers to issue fines are subject to certain safeguards, including a requirement for the penalty notice to be preceded by a notice of intent, for the opportunity to make representations against a proposed fine, and for information to be given about the right of appeal under the Act in relation to any penalty notice subsequently issued or the amount specified in that notice.

48 The 1998 Act included certain criminal offences relating to making a false statement in response to an information notice, obtaining or disclosing personal data without the data controller's consent and general offences relating to compliance with warrants etc and misconduct of the Commissioner's own officers. Most prosecutions were brought under section 55 of the 1998 Act, where a person knowingly or recklessly obtained, disclosed or procured the disclosure of, personal data without the data controller's consent. The maximum penalty was an unlimited fine. The Act 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 a small number of new offences to deal with emerging threats.

49 In June 2016, Dame Fiona Caldicott, the National Data Guardian for Health and Care published her Review of Data Security Consent and Opt-Outs[2] 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[3] and committed to create a new offence along these lines. The Act provides for such an offence in section 171.

Legal background

General processing

50 Convention 108 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.

51 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.

52 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.

53 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 appropriate exemptions.

54 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.

55 The GDPR was published in the Official Journal of the European Union[4] on 4 May 2016 and directly applies from 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

---

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

[3] UK Digital Strategy, Policy paper. 1 March 2017

[4] 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)

law. The Act therefore does not reproduce the text of the GDPR but instead exercises available derogations.

Law enforcement processing

56 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 above, however, the provisions in Part 3 of the Act apply to all processing – domestic and trans-national – for law enforcement purposes.

57 In accordance with the Government's Transposition Guidance[5], the approach taken in Part 3 of the Act 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.

Intelligence services processing

58 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.

59 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.

60 The main innovations in the modernised Convention 108 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

[5] Transposition Guidance: How to implement European Directives effectively

taken into consideration, the right to obtain information about the logic underlying the processing, and the right to object.

61 Article 9 of the modernised Convention 108 will continue to allow Parties to exempt controllers from some of these requirements for specified purposes. One such purpose is the protection of national security.

Parliamentary scrutiny

62 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]).

Territorial extent and application

63 Subject to minor exceptions, the Act extends and applies to the whole of the UK. Sections 188, 189 and 190 (representation of data subjects) apply and extend to England and Wales and Northern Ireland only. Section 199 (recordable offences) extends and applies to England and Wales only.

64 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 Act is consistent with the 1998 Act so in the Government's view, is also a reserved matter.

65 The subject matter of the 1998 Act is also a reserved matter under paragraph 40 of Schedule 3 to the Northern Ireland Act 1998.

66 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.

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

Commentary on provisions of Act

Part 1: Preliminary

Section 1: Overview

67 This section sets out the various Parts of the Act and is self-explanatory.

Section 2: Protection of personal data

68 The Act, together with the GDPR, makes provision about the processing of personal data. Article 1 of the GDPR declares that the regulation protects individuals' rights to data protection. While Chapter 2 of Part 2 concerns the GDPR, the Act extends to all personal data processing in the United Kingdom. This declaratory section does not create any new rights additional to those found in the Act and the GDPR, but provides a supplementary overview of the Act's focus on protecting individuals with regard to the processing of personal data. The section is otherwise self-explanatory.

Section 3: Terms relating to processing of personal data

69 This section defines key terms used in the Act.

70 Part 2 of the Act concerns general data and makes provision for those areas where the GDPR gives Member States discretion in their implementation. To fully understand the Act it is necessary to read it alongside the definitions found in the GDPR.

71 The Act adopts many of the definitions found in Article 4 of the GDPR and extends them to apply across the Act. In particular the following definitions are adopted:

Term	GDPR Definition	Act 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.	Subsections (2) and (3) extend the GDPR definition to apply across the Act.
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 Act.
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 Act.

72 The meaning of the terms "personal data", "processing", "controller" and "processor" within Parts 2 to 4 of the Act may be limited or modified by the regimes within those Parts. For example, the meaning of "controller" is modified in Chapter 2 of Part 2 for the purposes of that chapter (see section 6) and also limited by the scope of the Chapter 2 of Part 2 regime. Subsection (14) states that where such terms appear in Parts 5 to 7 of the Act – which contains cross-cutting provisions that apply to all of the regimes in Parts 2 to 4 of the Act – its meaning will depend on the applicable regime, except where otherwise provided. Generally, references in Parts 5 to 7 to the GDPR should be read as including the applied GDPR; and references in

Parts 5 to 7 to Chapter 2 of Part 2 should be read as including Chapter 3 of Part 2.

Part 2: General processing

Chapter 1: Scope and definitions

Section 4: Processing to which this Part applies

73 This section 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 the GDPR is limited by the Treaty on European Union and consistent data processing standards for all general data processing is desirable, Chapter 3 applies the same standards to types of processing that are not within the scope of EU law.

Chapter 2: The GDPR

Section 5: Definitions

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

Section 6: Meaning of "controller"

75 This section supplements the definition of "controller" found in Article 4(7) of the GDPR. This section 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 controller. This provision replicates section 1(4) of the 1998 Act.

Section 7: Meaning of "public authority" and "public body"

76 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).

77 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 purposes of Article 6(1)(e) and Article 37.

78 This section defines public authority and public body for the purpose of the GDPR and is largely consistent with the definition which existed in section 1(1) of the 1998 Act.

79 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 and to Scottish public authorities as defined by the Freedom of Information (Scotland) Act 2002. Subsection 1(c) provides a power for the Secretary of States to designate additional bodies as "public authorities" for the purposes of the GDPR by regulations.

80 Subsection (2) makes clear that a public authority or public body will only be regarded as such for the purposes of the GDPR when it is carrying out a task in the public interest or in the exercise of official authority vested in it. Conversely, where such a body is carrying out a non-public function, it is not treated as a public authority for the purposes of the GDPR As a result it may, in some circumstances, be able to rely on Article 6(1)(f) of the GDPR as a lawful basis for processing.

81 Subsection (3) provides that the authorities listed are not "public authorities" for the purposes

of the GDPR, even though they are (or may in future be) public authorities for the purposes of the 2000 Act or the Freedom of Information (Scotland) Act 2002.

82 Subsection (4) contains a power for the Secretary of State to specify that a body is not a public authority for the purposes of the GDPR, even if they are otherwise included by virtue of subsection (1)(a) or (b).

83 Subsection (5) provides that regulations under this section are subject to the affirmative resolution procedure.

Section 8: Lawfulness of processing: public interest etc

84 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 (the limitation in Article 6(3) notwithstanding). 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).

85 This section 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, a function conferred on a person by enactment or rule of law or an activity that supports or promotes democratic engagement. The list is similar to that contained in paragraph 5 of Schedule 2 to the 1998 Act. As the list is non-exhaustive, organisations whose processing activities are not listed in this section will still be able to rely on Article 6(1)(e) where those activities are carried out in the public interest or in the exercise of the controller's official authority. So, for example, a university undertaking processing of personal data necessary for medical research purposes in the public interest should be able to rely on Article 6(1)(e).

86 The term "democratic engagement" is intended to cover a wide range of political activities inside and outside election periods, including but not limited to: democratic representation; communicating with electors and interested parties; surveying and opinion gathering, campaigning activities; activities to increase voter turnout; supporting the work of elected representatives, prospective candidates and official candidates; and fundraising to support any of these activities.

Section 9: Child's consent in relation to information society services

87 Where an information society service chooses to rely on 'consent' as the basis for processing personal data, Article 8 of the GDPR sets the age of the data subject below which it is the parent's, not the child's, consent that they must obtain. 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 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 This section 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 section clarifies the position in relation to preventative and counselling services and provides that references to information society services in Article 8 of the GDPR do not include preventative and counselling services.

91 The 1998 Act did 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 did not contain a reference to information society services, as this concept was first defined in the E-commerce Directive (2000/31/EC).

Section 10: 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 or varying processing conditions or safeguards, and omitting conditions or safeguards added by regulations, as well as powers to make consequential amendments to this section. These regulations are subject to the affirmative resolution procedure.

101 This section does not reproduce all of the conditions previously 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

Section 11: Special categories of personal data etc: supplementary

102 This section 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) of the GDPR (obligations of professional secrecy etc.). Section 11(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 responsibility 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 Act in section 204.

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

Section 12: Limits on fees that may be charged by controllers

105 This section enables the Secretary of State to specify in regulations 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.

106 The Secretary of State may also 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.

Section 13: Obligations of credit reference agencies

108 This section 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.

Section 14: Automated decision-making authorised by law: safeguards

111 This section relates to Article 22 of the GDPR. It provides the safeguards that apply in relation to certain types of automated decision making.

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 (Article 22(2)(a));
- authorised by law to which the data controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests (Article 22(2)(b)); or
- based on the data subject's explicit consent (Article 22(2)(c)).

113 Decision making "based solely on automated processing" is not further defined in the GDPR. The Article 29 Working Party guidelines on automated decision-making suggest that a decision will be "based solely on automated processing" where there is no "meaningful" human involvement in the decision making process.[7]

114 "Profiling" is a new term. It is defined in Article 4(4) of the GDPR 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 Article 22(2)(b) of the GDPR does not require the law to expressly provide that a decision can be made based solely on automated processing before that decision can be taken on the basis of automated processing. It is enough that automated processing is a reasonable way of complying with a requirement, such as a regulatory obligation or licence condition. Such obligation may be provided in general terms, such as a requirement to maintain fraud and

[7] "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)". Available online: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

financial crime detection systems.

116 This section provides the "suitable measures to safeguard the data subject's rights, freedoms and legitimate interests" that apply where the automated decision making is authorised by law (see above).

117 Subsection (4) requires the data controller to inform the data subject within a reasonable time frame that a significant decision has been taken about the data subject based solely on automated processing. The data subject can request the data controller to reconsider the decision or take a new decision using human intervention within one month from being informed of the original decision.

118 Subsection (6) provides a signpost to Article 12 of the GDPR which confers powers, and places obligations, on controllers to whom this section applies.

119 Subsection (7) 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.

Section 15: Exemptions etc

120 Subsections (1) to (4) of this section are self-explanatory and signposts the relative restrictions to data subject rights under the GDPR.

121 Subsection (5) is a distinct signposting provision. National security and defence are outside the scope of EU law. Consequently, for example, 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 or defence is 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 sections 26 to 28. Where national security or is engaged, subsection (5) therefore signposts data controllers, processors and others to the applied GDPR scheme.

Section 16: Power to make further exemptions etc by regulations

122 This section provides the Secretary of State with the power to make regulations altering the application of the GDPR under Articles 6(3), 23(1) and 85(2), including adding or varying the derogations in Schedules 2 to 4 and omitting provisions subsequently added by regulations, as well as power to make consequential amendments to section 15.

123 Regulations made under this section are subject to the affirmative resolution procedure.

Section 17: Accreditation of certification providers

124 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 GDPR Certificates can be issued by the supervisory authority or by certification providers.

125 Under Article 43 of the GDPR, Member States must ensure any certification providers 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.

126 This section outlines the process and requirements for accrediting certification bodies to oversee the certification mechanisms outlined in Article 42.

127 Subsection (2) provides the conditions that the Commissioner must meet to accredit a person

as a certification provider.

128 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.

129 Subsection (4) provides for the validity of any accreditation carried out before publication of a notice under (2)(b) or (3)(b).

130 Subsection (5) introduces Schedule 5 which makes provision about reviews and appeals of decisions of the accreditation authorities.

131 Subsection (6) provides the national accreditation body with a power to charge fees in respect of its accreditation functions under the Act.

132 Subsection (7) outlines that the national accreditation body must provide information to the Secretary of State relating to the accreditation it carries out under the GDPR.

133 Subsection (8) defines "certification provider" as meaning a person which issues certification for the purposes of Article 42 of the GDPR. It also defines the national accreditation body as the same body as that in Article 4(1) of Regulation (EC) 765/2008, setting out the requirements for accreditation and market surveillance. In the United Kingdom, this is currently the United Kingdom Accreditation Service (UKAS).

134 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 section is likely to be in breach of the business and consumer protection provisions in the Business Protection from Misleading Marketing Regulations 2008 (S.I. 2008/1276) or the Consumer Protection from Unfair Trading Regulations 2008 (S.I. 2008/1277).

Section 18: Transfers of personal data to third countries

135 This section relates to transfers of personal data to third countries (countries or territories that are not Member States) and international organisations (as defined in Article 4 of the GDPR) under Article 49 of the GDPR.

136 Chapter V of the GDPR concerns transfers of personal data to third countries and international organisations. Article 45 permits such "international transfers" where the Commission has determined that the relevant third country or international organisation ensures an adequate level of protection (an "adequacy decision"). In addition, Article 46 permits international transfers subject to appropriate safeguards and Article 49(1) sets out other limited bases for transferring personal data to third countries or international organisations where there is neither a relevant adequacy decision nor appropriate safeguards in place. For example, Article 49(1)(d) permits transfers necessary for important reasons of public interest.

137 Article 49(4) enables Member States to create domestic law to specify important reasons of public interest, for the purposes of Article 49(1)(d). Article 49(5) also enables Member States to create domestic law to put restrictions on international transfers, for important reasons of public interest and where there is no adequacy decision in place. This section provides regulation-making powers for these circumstances.

138 Subsection (1) deals with the first circumstance and is similar to the order-making powers previously provided under paragraph 4 of Schedule 4 to the 1998 Act. It allows the Secretary of State to specify through regulations circumstances in which international transfers of personal data are or are not taken to be necessary for important reasons of public interest.

139 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.

140 Subsection (3) provides that regulations made under this section are subject to the affirmative resolution procedure, save for where the Secretary of State has made an urgency statement in respect of them, in which case the "made affirmative" resolution procedure (rather than the affirmative resolution procedure) will apply.

141 Subsection (4) explains that any urgency statement must set out the reasons why the Secretary of State considers it necessary for certain regulations to come into force without delay.

Section 19: Processing for archiving, research and statistical purposes: safeguards

142 Article 89(1) of the GDPR requires appropriate safeguards for the processing of personal data in support of archiving, scientific or historical research purposes and statistical purposes. The 1998 Act required those relying on the "research exemptions" in section 33 of that Act to comply with certain safeguards to ensure that personal data would not be processed by researchers to support measures or decisions with respect to particular individuals, and would not be processed in a way likely to cause substantial damage or distress to any data subject. This section replicates these safeguards.

143 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.

144 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.

145 Subsection (3) 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 personal data is processed to support a decision being made about the subject, unless it is carried out for the purposes of approved medical research. Subsection (4) defines the meaning of "approved medical research".

Section 20: Meaning of "court"

146 References to "court" in the GDPR are likely to include "tribunal" (as defined in the Act in section 205). For consistency across the Act, and to minimise uncertainty, Chapter 2 of Part 2 uses the construction "court or tribunal" where applicable, with the effect that "court" in Chapter 2 of Part 2 has a narrower meaning than "court" in the GDPR, as it does not include "tribunal". Section 20 therefore disapplies, for the term "court", the general provision in section 5(1) that terms in the GDPR and Chapter 2 of Part 2 have the same meaning as each other.

Chapter 3: Other general processing

Section 21: Processing to which this Chapter applies

147 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.

148 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 by competent bodies for law

enforcement purposes or by the intelligence services. Those types of processing are covered by their own regimes in Parts 3 and 4 of this Act.

149 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 (as amended by the 2000 Act), but is not covered by the GDPR, so equivalent provision is needed.

150 Definitions of "automated or 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.

Section 22: Application of the GDPR to processing to which this Chapter applies

151 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) extends the application of Chapter 2 to this Chapter.

152 Subsections (3) defines "the applied Chapter 2".

153 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.

154 Subsection (5) provides for consistency in interpretation between the applied GDPR and the applied Chapter 2 and the "real" GDPR and "real" Chapter 2.

Section 23: Power to make provision in consequence of regulations related to the GDPR

155 This section provides a delegated power to amend certain parts of the Act relating to processing within scope of Part 2 Chapter 3 of the Act to mirror changes "relating to the GDPR" made using section 2(2) of the European Communities Act 1972. Such provision would stand apart from the Act, so the Act's mechanisms to automatically apply changes to Chapter 2 of Part 2 to Chapter 3 of Part 2 would not be engaged.

Section 24: Manual unstructured data held by FOI public authorities

156 Although section 21 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.

157 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.

158 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.

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

160 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.

Section 25: Manual unstructured data used in longstanding historical research

161 This section 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 the purposes of measures or decisions with respect to a particular data subject, or in a way that causes, or is likely to cause, substantial damage or distress to the subject. The limit of 24 October 1998 is consistent with the 1998 Act.

162 This section also provides that exemptions in section 24 on manual unstructured data held by FOI public authorities also apply.

Sections 26 to 28: National security and defence exemption

163 These sections create an exemption from certain provisions in the applied GDPR scheme and in Parts 5, 6 and 7 of the Act if that exemption is required for the purpose of safeguarding national security or for defence purposes. The provisions that may be disapplied in such circumstances are listed in subsection (2) of section 26 and include most of the data protection principles, the rights of data subjects, certain obligations on data controllers and processors, and various enforcement provisions.

164 Section 26 provides for an exemption similar to that in section 28 of the 1998 Act where this is required for the purpose of safeguarding national security. Schedule 7 to the 1998 Act provided further exemptions to the subject information provisions, including at paragraph 2, when they would be likely to prejudice the "combat effectiveness" of the armed forces.

165 The "defence purposes" element of section 26 is intended to ensure the continued protection, security and capability of the armed forces, and the civilian staff that support them, not just their combat effectiveness. The following are examples of processing activities which might be considered defence purposes requiring the protection of the exemption:

- collection, consideration and utilisation of military or other defence related intelligence in support of current and future military operations;
- collation of personal data to assist in assessing the capability and effectiveness of armed forces personnel, including performance of troops;
- collection and storage of information, including biometric details, necessary to maintain the security of defence sites, supplies and services;
- management of data relating to former armed forces personnel who hold a reserve liability;
- sharing of data with coalition partners to support them in maintaining their security, capability and effectiveness of their armed forces.

166 This is not an exhaustive list, and the application of the exemption should only be considered

in specific cases where the fulfilment of a specific data protection right or obligation is found to place the security, capability or effectiveness of UK defence activities at risk.

167 As was the case under the 1998 Act, a Minister of the Crown (as defined in section 27(10)) may certify that an exemption is required in respect of specified personal data or processing for the purpose of safeguarding national security. Section 27(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 the national security exemption applies to the specified data processing. Section 130 below makes provision for the publication of such ministerial certificates.

168 Any person directly affected by the issuing of any certificate may appeal 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 (section 27(3)). Such an appeal would be heard by the Upper Tribunal which would apply judicial review principles when determining the appeal. In applying such principles the Upper Tribunal would be able to consider a wide range of issues, including necessity, proportionality and lawfulness. This would enable, for example, the Upper Tribunal to consider whether the decision to issue the certificate was reasonable, having regard to the impact on the rights of data subjects and balancing the need to safeguard national security.

169 Section 28 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 and defence purposes. In each instance, alternative security measures appropriate to the risk must be implemented.

Part 3: Law enforcement processing

Chapter 1: Scope and definitions

Section 29: Processing to which this Part applies

170 This overview section sets out the scope of the processing to which Part 3 of the Act applies. 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 section 3(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 (but see section 26).

Sections 30 to 33: Definitions

171 These sections define terms used in Part 3. There are also additional definitions in sections 3 and 205 which are relevant to the Act as a whole. The definition of "personal data" in section 3(2) is such that anonymised data falls outside the provisions of this Part as does data in relation to an individual who has died.

172 Schedule 7 lists the principal 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 law enforcement 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 law enforcement functions, for example the Department for Work and Pensions in relation to benefit fraud or the Home Office in relation to immigration crime. Where a UK government department, the Scottish Ministers, the Welsh Ministers or a Northern Ireland department do not have responsibilities which involve the processing of personal data for law enforcement purposes, these entries in paragraphs 1 to 4 of Schedule 7 will not impose obligations on those departments or Ministers under this Part.

173 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. Section 30(1)(b) provides for a catch-all provision to capture other persons (that is, office holders or organisations) exercising statutory functions for any of law enforcement purposes, for example local authorities when prosecuting trading standards offences or the Environment Agency when prosecuting environmental offences. It does not, however, apply to an individual or organisation (such as the Royal Society for the Prevention of Cruelty to Animals) 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 Act. This reflects Recital 14 of the LED, which acknowledges that the activities of agencies dealing with national security issues fall outside the scope of the Directive.

174 Section 30(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).

175 The definition of "law enforcement purposes" in section 31 sets the boundaries to which the data protection regime in Part 3 of the Act applies. Not all processing of personal data by a competent authority will be for law enforcement purposes. This is because where a controller determines that the processing will take place for another purpose, 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).

176 Section 32 defines the terms "controller" and "processor" for the purposes of Part 3. The controller (which includes employees of the controller) determines the purpose and means of processing; or alternatively their responsibility may be set out in law. The definition of an "employee" in section 33(2) ensures that, in this context, police officers and special constables (who are office holders rather than employees) are treated as an extension of their chief officer.

177 Where two or more controllers act together as controllers to decide the purpose and means of any data processing they are known as "joint controllers". For example, the Police National Computer is managed on behalf of all police forces in the UK with individual chief constables jointly determining the purposes and means of the processing of the personal data held on the database. In this situation, the chief constables will be acting as joint controllers.

178 Processors act on behalf of the controller. Similar to the 1998 Act, section 32(3) makes clear a processor does not include an employee of the controller.

Chapter 2: Principles

Section 34: Overview and general duty of controller

179 This section sets out an overview of 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 (section 34(3)). The principles here are analogous to the first, second, third, fourth, fifth and seventh principles provided for in the 1998 Act; the sixth and eight principles of that Act are covered separately under Chapters 3 and 5 of this Part.

Section 35: The first data protection principle

180 The first principle (section 35) 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 manner. This omission recognises the inherent sensitivities of processing for the law enforcement purposes by competent authorities, particularly where transparency would undermine or compromise covert techniques and capabilities, and/or sensitive or covert operations including, for example, where investigatory powers under the Regulation of Investigatory Powers Act 2000 or Investigatory Powers Act 2016 are engaged.

181 "Lawful" processing means authorised by either statute, common law or royal prerogative. 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.

182 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.

183 Article 10 of the LED generally prohibits the processing of "special categories of personal data" unless specific circumstances apply.

184 Section 35 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 "strictly necessary" 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. The Article 29 Working Party has opined "that the term "strictly necessary" in Article 10 [of the LED] has to be understood as a call to pay particular attention to the necessity principle in the context of processing special categories of data, as well as to foresee precise and particularly solid justifications for the processing of such data". Section 42 makes further provision in respect of such appropriate policies in respect of sensitive processing.

Section 36: The second data protection principle

185 The second principle (section 36) 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 in connection with the prosecution of a criminal offence, whereas the police working alongside the prosecutor would be processing the personal data in connection with the investigation of the offence.

Section 37: The third data protection principle

186 The third principle (section 37) 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" was also used (undefined) in the 1998 Act; Commissioner guidance provided that in practice this term meant that controllers should ensure that:

- they hold personal data about an individual that is sufficient for the purpose it is being held for in relation to that individual; and
- they do not hold more information than is needed for that purpose.

Section 38: The fourth data protection principle

187 The fourth principle (section 38) 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. Section 38(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.

Section 39: The fifth data protection principle

188 The fifth principle (section 39) 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 section 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.

Section 40: The sixth data protection principle

189 The sixth principle (section 40) requires personal data to be processed in a secure manner. The Commissioner's guidance stipulates that, in practice, this means that the controller must have appropriate security to prevent the personal data they hold being accidentally or deliberately compromised. In particular, the 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.

Section 41: Safeguards: archiving

190 This section provides safeguards in relation to the processing of personal data for a law enforcement purpose where the processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes. Such processing is prohibited where it is carried out in relation to a measure or decisions in respect of a particular data subject or it is likely to cause substantial damage or substantial distress to a data subject.

Section 42: Safeguards: sensitive processing

191 Section 35 requires controllers, in certain circumstances, to have an appropriate policy document in place. Section 42 makes further provision in respect of such documents.

Chapter 3: Rights of the data subject

Section 43: Overview and scope

192 This section provides an overview the rights of data subjects conferred by Chapter 3 of 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.

193 Subsections (3) provides that the subject access rights and the rights to rectification, erasure and restriction of processing do not apply in relation to the processing of "relevant personal data" (as defined in subsection (4)) in the course of a criminal investigation or criminal proceedings. Instead, access to such "relevant personal data" will be governed by the appropriate legislation covering the disclosure of information in criminal proceedings, such as (in England and Wales) the Criminal Procedure and Investigation Act 1996. This provision only applies where the judge or other judicial authority is the controller and the relevant personal data is contained in a judicial decision or in other documents which are created

during a criminal investigation or proceedings and made by or on behalf of the judge or judicial authority. For example, the "relevant personal data" may be contained in judge's notes made whilst providing judicial approval under section 32A of the Regulation of Investigatory Powers Act 2000 during the investigation or in a pre-sentencing report commissioned by the judge in the course of the proceedings. In such instances, the data subject's rights set out in sections 44 to 48 in respect of such data will be diverted to the relevant domestic legislation governing disclosure of such data by virtue of this provision. Where a competent authority is commissioned by a court or other judicial authority to create a document, the provisions in subsection (3) extend to that document and the personal data contained within it. The original personal data processed by the competent authority used to inform the document will remain subject to the provisions in sections 44 to 48.

Section 44: Information: controller's general duties

194 This section 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.

195 Subsection (2) sets out additional information which a controller must provide "in specific cases" to a data subject to enable the data subject to exercise his or her subject access rights. An example of such a case could be where the personal data is collected without the data subject being aware and to inform the data subject would not, for example, prejudice an on-going investigation.

196 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.

Section 45: Right of access by the data subject

197 This section 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).

198 As with the previous section, the subject access rights conferred by this section 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 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 why they have restricted the access rights of a data subject and make the record available to the Commissioner (if requested).

Sections 46 to 48: Data subject's rights to rectification or erasure etc

199 These sections enable a data subject to ask for data to be corrected, erased or the processing of that data to be restricted. The data subject may challenge the processing of the data directly to the controller. Correction can include adding to incomplete personal data, for example by means of the provision of further information. 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 controller may restrict the right to rectification where, for example, it would obstruct an investigation, such as a request to rectify the content of a witness statement. 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.

200 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 by applying strict access controls. The fact that the processing of the personal data is restricted should be indicated on the system, for example, through flagging.

201 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 section 48.

202 Where this restriction has been exercised by the controller, the data subject may lodge a complaint with the Commissioner. Sections 165 and 166 make further provision in respect of complaints by data subjects.

203 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).

Sections 49 and 50: Automated individual decision-making

204 Section 49 prohibits the controller from making a "significant decision" based solely on automated processing unless the decision is required or authorised by law. A "significant decision" is one which result in adverse legal effects concerning the data subject or significantly affects the data subject. Where the controller is required or authorised by law to make a significant decision, section 50 sets out the safeguards that will apply to such a decision (which is defined as a "qualifying significant decision"). Such safeguards include a duty on the controller to inform the data subject of an automated decision and his or her right to request (within a month of being notified) that the controller reconsider the decision or take a new decision on the basis of human intervention. These provisions are in relation to fully automated decision-making and not to automated processing. Automated processing (including profiling) is when an operation is carried out on data without the need for human intervention. It is regularly used in law enforcement to filter down large data sets to manageable amounts for a human operator to then use. Automated decision-making is a form of automated processing and requires the final decision to be made without human interference.

205 The Article 29 working party guidelines on automated decision-making for the purposes of the GDPR (but equally applicable here) suggests that a decision will be "based solely on

automated processing" unless the level of human intervention "is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision."

206 In practice, currently automated decision-making that leads to an adverse outcome is rarely used in the law enforcement context and is unlikely to have any operational implications.

Sections 51 to 54: Supplementary

207 These sections make supplementary provisions about the exercise of data subjects' rights through the Commissioner. 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, in contrast to the 1998 Act, section 52(5) provides that the controller must respond to a subject access request free of charge (the 1998 Act permitted data controllers to charge a fee of up to £10).

208 Section 53, 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, or where the controller has provided the data subject with their personal data through an alternative disclosure mechanism. 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

Section 55: Overview and scope

209 This overview section is self-explanatory.

Sections 56 to 65: General obligations

210 This Chapter provides for obligations on controllers and processors. Sections 56 and 57 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 section 64).

211 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 considerations 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 from the outset. 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 consequences of a

data breach, potential for fraud or misuse of the data, damage to the data subject's reputation) linked to processing must be considered when applying appropriate technical and organisational safeguards.

212 Section 58 establishes the responsibilities for joint controllers. Where two or more competent authorities jointly determine the purposes and means of the processing of personal data they will be "joint controllers" for the purposes of Part 3. This provision further requires that 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. The definition of joint controllers used here extends the concept of "controllers in common" used in the 1998 Act; this is because any agreement between joint controllers must have an unambiguous apportionment of responsibilities under the Act, and set-out which controller will be responsible for each function.

213 Sections 59 and 60 provide for the use by a controller of a processor to carry out processing of personal data on behalf of the controller. In particular, a controller may only use a processor where the processor is able to guarantee 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.

214 There is also a requirement that the processing by the processor is governed by a contract or other legal act, which is binding on the processor with regard to the controller. Section 58(5) and (6) specify a number of provisions that will ensure the lawfulness of the processing that must be included in such a contract including a duty of confidentiality.

215 Overall the controller will need, if requested, to demonstrate its own processing or that done on its behalf by a processor is compliant with the requirements of this Part. Any arrangement between the controller and processor will need to reflect these requirements.

216 To that end, section 61 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.

217 Section 62 imposes logging requirements. Such requirements were 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). Self-monitoring includes internal disciplinary proceedings with a competent authority. The Independent Office for Police Conduct (formally the Independent Police Complaints Commission) has 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 details of when the record was accessed and, where possible, by whom, which would assist the investigation possibly leading to criminal or disciplinary action and possible dismissal.

218 Many automated systems have existing logging capabilities; however, there is a requirement within the section 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 section 62, must apply by 6 May 2023. This is provided for in paragraph 14 of Schedule 20 to the Act.

219 Section 64 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).

220 Where an impact assessment has indicated there is a high risk associated with the processing, section 65 requires 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.

Section 66: Obligations relating to security

221 These sections 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.

Sections 67 and 68: Obligations relating to personal data breaches

222 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 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 of becoming aware of it and give details as to how they are mitigating that risk.

223 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, section 68 enables controllers to restrict the data subject's right by withholding notice of a data breach in certain circumstances where notifying a data subject would reveal the existence of the data to the detriment of an ongoing criminal investigation etc.

Sections 69 to 71: Data protection officers

224 These sections provide for the appointment and the tasks of data protection officers ("DPO"). There was no 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). Irrespectively, the DPO will need to be suitably senior and resourced to be able to undertake his or her duties.

225 Section 71 mandates the controller to make the DPO responsible for the specified tasks set out in subsection (1). Overall the role of the DPO 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

Section 72: Overview and interpretation

226 The transfer of personal data to a third country (as defined in section 33(7)) 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 section 30, (except in the case of section 77 which provides for the transfer of data in specific circumstances to a person who does not carry out such functions).

227 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.

Sections 73 to 76: General principles for transfers

228 Section 73 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. As of May 2018, 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).

229 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 section 75 or 76, which govern transfers based on appropriate safeguards and specific circumstances, are fulfilled.

230 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.

231 Where no adequacy decision or appropriate safeguards exist, section 76 provides that a transfer or a category of transfers could take place 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 Commissioner on request in order to monitor the lawfulness of the transfer.

Section 77: Transfers of personal data to persons other than relevant authorities

232 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.

233 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 Act. 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.

Section 78: Subsequent transfers

234 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

Section 79: National security: certificate

235 This section provides that a Minister of the Crown (as defined in subsection (12)) may certify that, for the purposes of sections 44(4), 45(4), 48(3) and 68(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. Section 130 below makes provision for the publication of such ministerial certificates.

236 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)). Such an appeal would be heard by the Upper Tribunal which would apply judicial review principles when determining the appeal. In applying such principles, the Upper Tribunal would be able to consider a wide range of issues, including necessity, proportionality and lawfulness. This would enable, for example, the Upper Tribunal to consider whether the decision to issue the certificate was reasonable, having regard to the impact on the rights of data subjects and balancing the need to safeguard national security.

Section 80: Special processing restrictions

237 This section provides that where any domestic restrictions (other than those provided for by or under this Act) 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.

Section 81: Reporting of infringements

238 This section 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

Sections 82 to 84: Processing to which this Part applies and definitions

239 Section 82 applies the provisions in Part 4 of the Act to personal data controlled by an intelligence service (the Security Service, Secret Intelligence Service and Government Communications Headquarters).

240 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; and
  - 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.

241 Section 83 defines "processor" and "controller" for the purposes of intelligence service processing under Part 4.

242 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.

243 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.

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

245 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 section 3(7)). A structured filing system is one containing records relating to data subjects held in a sufficiently systematic, structured way as to allow ready access to specific information about those subjects. Files which are not structured according to specific criteria do not fall within the scope of this Part.

246 Section 84 defines other expressions used in this Part.

Chapter 2: Principles

Sections 85 to 91: Data protection principles

247 These sections 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.

248 The first principle (section 86) 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 section 86(7)) are stricter and are set out in Schedule 10. Section 86(3) confers a regulation-making power (subject to the affirmative procedure) on the Secretary of State to add to conditions in Schedule 10. It also establishes a power to omit conditions added by regulations made under this section.

249 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).

250 The principle of transparency requires 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.

251 The second principle (section 87) 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.

252 The third principle (section 88) 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.

253 The fourth principle (section 89) 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.

254 The fifth principle (section 90) requires that personal data undergoing processing be kept for no longer than is necessary. To comply with this principle, controllers should establish time limits for erasure, or for periodic review. Similarly to the previous position under the 1998 Act, this section does not specify minimum or maximum periods for the retention of data. In practice, to comply with the fifth principle, controllers should review the length of time they retain personal data; consider the purpose or purposes for which they hold information 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.

255 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.

256 The sixth principle (section 91) 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

Section 92: Overview

257 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; the right to information about decision making; the right to object to processing; and the rights to rectification and erasure of personal data.

Section 93: Right to information

258 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.

259 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.

Sections 94 and 95: Right of access

260 These sections 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 Act, under these provisions a controller may charge a reasonable fee before responding to subject access requests.

261 Sections 94(6) and 95(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.

262 If a controller does not comply with a request under section 94(1) the data subject who made the request can apply to the High Court (or, in Scotland, the Court of Session) under section 94(11) for an order requiring the controller to comply with the request. Under section 94(12) a

court may make an order under subsection (11) in relation to a joint controller whose responsibilities are determined in an arrangement under section 104 only if the controller is responsible for compliance with the obligation to which the order relates. In practice, this means that any order made by the court must be consistent with the responsibilities assigned to a controller under a joint controller agreement.

263 Section 95 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.

Sections 96 to 98: Rights related to decision-making

264 Sections 96 and 97 provide for a general right for data subjects 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 law. In the case of an automated decision being taken when required or authorised by law, the 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 (section 97).

265 Section 98 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).

Section 99: Right to object to processing

266 This section 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.

267 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). Under subsection (6) a court may make an order under subsection (5) in relation to a joint controller whose responsibilities are determined in an arrangement under section 104 only if the controller is responsible for compliance with the obligation to which the order relates. In practice, this means that any order made by the court must be consistent with the responsibilities assigned to a controller under a joint controller agreement.

Section 100: Right to rectification or erasure

268 This section 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.

269 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.

270 This section 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.

271 Subsection (5) provides that a court may make an order under this section in relation to a joint controller whose responsibilities are determined in an arrangement under section 104 only if the controller is responsible for carrying out the rectification, erasure or restriction of processing that the court proposes to order. For example, if the court intends to make an order requiring data within a certain database to be rectified, and the joint controller arrangement provides that one joint controller is responsible for amending that database, then the court could only make an order in relation to that responsible joint controller.

Chapter 4: Controller and processor

Section 101: Overview

272 This overview section is self-explanatory.

Sections 102 to 106: General obligations of controllers and processors

273 These sections provide for obligations on controllers and processors.

274 Sections 102 and 103 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.

275 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.

276 Section 104 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.

277 Section 105 provides that 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 (section 106).

Section 107: Security of processing

278 This section 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.

Section 108: Communication of personal data breach

279 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 a data subject or data subjects, this section 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.

280 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.

281 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

Section 109: Transfers of personal data outside the United Kingdom

282 This section 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, 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

Sections 110 and 111: National security

283 Section 110 creates an exemption from certain provisions in the Act 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 Act and include most of the data protection principles, the rights of data subjects, certain obligations on controllers and processors, and various enforcement provisions. This exemption mirrors the position previously provided for in section 28 of the 1998 Act.

284 Section 111 provides that, as before 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. Section 130 below makes provision for the publication of such ministerial certificates.

285 These provisions allow departure from certain requirements of the Act 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.

286 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. Such an appeal would be heard by the Upper Tribunal which would apply judicial review principles when determining the appeal. In applying such principles the Upper Tribunal would be able to consider a wide range of issues, including necessity, proportionality and lawfulness. This would enable, for example, the Upper Tribunal to consider whether the decision to issue the certificate was reasonable, having regard to the impact on the rights of data subjects and balancing the need to safeguard national security.

Sections 112 and 113: Other exemptions

287 There are some other circumstances where the principles and rights provided for in the Act may conflict with other public interests or individual rights. Section 112 introduces Schedule 11, which provides for an exemption from certain provisions of the Act 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.

288 Section 113 provides for a power for the Secretary of State, by regulations (subject to the affirmative procedure) to amend Schedule 11 by adding further exemptions from the provisions of Part 4 or by omitting exemptions so added by regulations.

Part 5: The Information Commissioner

Section 114: The Information Commissioner

289 This section 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.

Section 115: General functions under the GDPR and safeguards

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

291 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.

292 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.

Section 116: Other general functions

293 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.

294 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. Section 3 provides a definition of the Convention.

Section 117: Competence in relation to courts etc

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

296 This section 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.

Section 118: Co-operation and mutual assistance

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

298 Schedule 14 to the Act provides further details about such functions in relation to the LED and Convention 108.

Section 119: Inspection of personal data in accordance with international obligations

299 This section allows 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. It is similar to section 54A of the 1998 Act, but rather than listing specific systems, it covers any such obligation.

300 Subsections (2) to (5) further describe the power of inspection, when it is exercisable, and a requirement to give prior notice, unless urgent.

301 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.

Section 120: Further international role

302 This section creates an obligation on the Commissioner to engage with third countries and international organisations. As set out in subsection (1), this obligation 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.

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

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

305 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.

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

Section 121: Data-sharing code

307 This section places an obligation on the Commissioner to publish and keep under review a data sharing code of practice. It replaces a similar requirement in section 52A of the 1998 Act.

308 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.

309 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.

Section 122: Direct marketing code

310 This section places the Commissioner under a duty to publish and keep under review a direct marketing code of practice. It replaces a similar requirement in section 52AA of the 1998 Act.

311 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 (S.I. 2003/2426) ("PECR"). When deciding what constitutes good practice, the Commissioner must have regard to the interests of data subjects and others.

312 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.

Section 123: Age-appropriate design code

313 This section places an obligation on the Commissioner to publish and keep under review an age-appropriate design code of practice.

314 Subsections (1) and (2) require the code to contain guidance on standards of age appropriate design for online services which are likely to be accessed by children. The Commissioner can also make amendments to the code or prepare a replacement code should this be necessary.

315 Subsection (3) requires that in preparing the code the Commissioner must consult the

Secretary of State and other such persons as the Commissioner considers appropriate, including children, parents, persons who represent the interests of children, child development experts and trade associations.

316 Subsection (4) requires that in preparing the code the Commissioner must take into account the fact that children have different needs at different ages. The Commissioner must also take into account the United Kingdom's obligations under the United Nations Conventions on the Rights of the Child.

317 Subsections (5) and (6) allow the Commissioner to include transitional provisions or savings in the code, but require that any transitional provisions included in the initial code cease to have effect within a year of the code coming into force.

318 Subsection (7) outlines definitions for "age-appropriate design", "information society services", "relevant information society services", "standards of age-appropriate design of relevant information society services", "trade association" and "the United Nations Convention on the Rights of the Child".

Section 124: Data protection and journalism code

319 This section requires the Information Commissioner to prepare a code of practice giving guidance about the processing of personal data for the purposes of journalism.

Section 125: Approval of codes prepared under sections 121 to 124

320 This section sets out the process by which the Secretary of State must seek the approval of Parliament for codes prepared under sections 121, 122, 123 and 124.

Section 126: Publication and review of codes issued under section 125(4)

321 This section sets out the process the Commissioner must follow when publishing a code prepared under section 125 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 sections 121(2), 122(2), 123(2) and 124(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.

Section 127: Effect of codes issued under section 125(4)

322 This section sets out the legal effect of codes published under section 125. It states that a code issued under section 125(3) is admissible in evidence in legal proceedings; and that a court or tribunal and the Information Commissioner must take a relevant provision of the code into account when determining a question arising in proceedings or in connection with the carrying out of the Commissioner's functions under the data protection legislation respectively.

Section 128: Other codes of practice

323 This section 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 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).

Section 129: Consensual audits

324 This section permits the Commissioner, with the consent of a data controller or processor, to carry out an assessment of whether the controller or processor is complying with good practice. It replaces similar provision in section 51(7) of the 1998 Act.

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

326 Subsection (3) defines the meaning of "good practice in the processing of personal data" by reference to section 128.

Section 130: Records of national security certificates

327 This section requires a Minister of the Crown who issues a certificate under sections 27, 79 or 111 to send a copy of the certificate to the Information Commissioner, who must publish a record of the certificate.

328 Under subsection (4) the Commissioner must not publish the text, or part of the text, of the certificate if the Minister determines, and has so advised the Commissioner, that to do so would be against the interests of national security, contrary to the public interest or might jeopardise the safety of any person.

329 Under subsections (5) and (6) the Commissioner must keep the record of the certificate available to the public while the certificate is in force and if a Minister of the Crown revokes a certificate the Minister must notify the Commissioner.

Section 131: Disclosure of information to the Commissioner

330 This section 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. The Commissioner has functions under the data protection legislation (as defined in section 3(9)) and also other functions which have been conferred by domestic legislation. For example, the Commissioner has regulatory functions under PECR, the Environmental Information Regulations 2004 (S.I. 2004/3391), the INSPIRE Regulations 2009 (S.I. 2009/3157), the Re-use of Public Sector Information Regulations 2015 (S.I. 2015/1415), the 2000 Act, the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (S.I. 2016/696), and Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

331 Subsection (2) clarifies that nothing in this section authorises the making of a disclosure which is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.

Section 132: Confidentiality of information

332 Subsection (1) of this section prohibits 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 the course of, or for the purposes of, the discharging of the Commissioner's functions unless made with lawful authority.

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

334 Subsection (3) establishes that it is an offence to knowingly or recklessly disclose information without lawful authority.

Section 133: Guidance about privileged communications

335 This section 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 section 143 (restrictions on information notices), section 147 (restrictions on assessment notices), paragraph 11 of Schedule 15 (powers of entry and inspection) or under equivalent provisions in other enactments (as defined in section 205).

336 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.

337 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).

338 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).

Section 134: Fees for services

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

Section 135: Manifestly unfounded or excessive requests by data subjects etc

340 This section is concerned with manifestly unfounded or excessive requests by data subjects and data protection officers.

341 Subsection (1) gives the Commissioner a discretion to charge a data subject or a data protection officer a fee for dealing with a manifestly unfounded or excessive request or to refuse that request.

342 Subsections (1) and (3) apply only in relation to cases which are outside the scope of the GDPR by virtue of subsection (4).

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

344 Subsection (3) requires the Commissioner to demonstrate that a request is excessive or unfounded.

Section 136: Guidance about fees

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

- section 134 in relation to fees for services;
- section 135 in relation to manifestly unfounded or excessive requests by data subjects or data protection officers; or
- Article 57(4) of the GDPR where requests which are within scope of that Regulation are manifestly unfounded or excessive.

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

Section 137: Charges payable to the Commissioner by controllers

347 This section 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.

348 This and the following section 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 Act to allow the new charges to be in place in time of the GDPR coming into force in May 2018. In particular, the Data Protection (Charges and Information) Regulations 2018 (S.I. 2018/480) were made using the powers conferred by the Digital Economy Act 2017 on 11 April 2018 and will come into force on 25 May 2018. Paragraph 26 of Schedule 20 to this Act makes transitional provision.

Section 138: Regulations under section 137: supplementary

349 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 before making regulations under section 137. Pursuant to section 182 the Secretary of State must also consult the Commissioner and such other persons as the Secretary of State considers appropriate.

350 The section 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 section 137 are subject to the affirmative procedure.

Section 139: Reporting to Parliament

351 Subsection (1) requires the Information Commissioner to produce a general report annually on the carrying out of the Commissioner's functions, lay it before Parliament and publish it. This section largely replicates section 52(1) of the 1998 Act.

352 Subsection (2) explains that a report must include an annual report of its activities as required by Article 59 of the GDPR.

353 Subsection (3) provides that the Commissioner can also lay other reports before the Houses of Parliament.

Section 140: Publication by the Commissioner

354 Where the Commissioner is under a duty to publish a document, this section provides that it can be published in any way that the Commissioner considers appropriate.

Section 141: Notices from the Commissioner

355 This section outlines the different ways in which the Commissioner may give a notice under this Act. This provision largely replicates section 65 of the 1998 Act.

Part 6: Enforcement

Section 142: Information notices

356 This section makes provision about information notices. An information notice can be used to require a controller, a processor or any other person to provide the Commissioner with

specified information within a certain time period.

357 Subsection (1) provides the Commissioner with a power to give an information notice.

358 Subsection (2) provides that the information notice must explain why the information is needed and whether it is given under subsection (1)(a), (b)(i) or (b)(ii).

359 Subsection (3) provides that the notice may include requirements about the information to be provided and how and when that information should be provided.

360 Subsection (4) requires an information notice to provide details about rights under sections 162 and 164 (appeals etc) and the consequences of a failure to comply with it.

361 Subsection (5) provides that an information notice must not require compliance with the measures in the notice before the end of the period in which an appeal could be brought.

362 Subsection (6) provides that if an appeal is brought, the person concerned need not comply with the information notice until the appeal has been withdrawn or decided.

363 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 to be provided. In these circumstances, however, the information notice must allow the person concerned at least 24 hours to provide the information requested.

364 Subsection (8) permits the Commissioner to cancel an assessment notice by written notice to the person to whom it was given.

Section 143: Information notices: restrictions

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

366 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 section 174 explaining why it would be justified.

367 Subsection (2) provides that an information notice does not require a person to give information to the Commissioner to the extent that requiring the person to do so would involve an infringement of the privileges of either House of Parliament.

368 Subsections (3) to (5) 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 under that legislation.

369 Subsection (6) provides that an information notice cannot compel a person to provide information that would expose them to proceedings for the commission of an offence, except in relation to the offences in this Act and the other offences listed in subsection (7). Where an information notice is served on the representative of a controller or processor who is based outside the UK, subsection (9) makes it clear that the representative is not required to provide information that would incriminate the controller or processor.

370 Subsection (8) provides that an oral or written statement provided in response to an information notice cannot be used as evidence in criminal proceedings brought under this Act (except where the proceedings relate to the offence in section 144 (false statements made in response to an information notice)) unless in the proceedings the defendant gave evidence which was inconsistent with the statement, and evidence relating to the statement is cited by

the person or a question relating to it is asked by the person or on their behalf.

Section 144: False statements made in response to information notices

371 This section makes it an offence for a person to intentionally or recklessly make a false statement in response to an information notice and replicates the offence in section 47(2) of the 1998 Act.

Section 145: Information orders

372 This section provides powers for the Commissioner to ask a court to order a person to comply with an information notice. Where a person has failed to comply with an information notice (given under section 142), the Information Commissioner may seek a court order requiring the person to provide the information referred to in the notice or other information which the court is satisfied the Commissioner requires, having regard to the original statement, in the notice, as to why information is required. Failure to comply with an information order may put the person at risk of proceedings for contempt of court.

Section 146: Assessment notices

373 This section empowers the Commissioner to give assessment notices. It replaces the provisions on assessment notices in section 41A of the 1998 Act.

374 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.

375 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 or observe processing that takes place on the premises, or, assisting the Commissioner to view certain documents or other information.

376 Subsection (4) requires the assessment notice to set out the times at which each requirement in the notice must be complied with.

377 Subsection (5) requires an assessment notice to provide information about rights under sections 162 and 164 (appeals etc) and the consequences of a failure to comply with it.

378 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.

379 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.

380 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.

381 Subsection (9) provides that, in certain circumstances, the Commissioner may require a person to comply with an assessment notice in less than 7 days, including with immediate effect.

382 Subsection (10) permits the Commissioner to cancel an assessment notice by written notice to the controller or processor to whom it was given.

383 Subsections (11) and (12) are self-explanatory.

Section 147: Assessment notices: restrictions

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

385 Subsection (1) provides that an assessment notice does not require a person to do something to the extent that requiring the person to do so would involve an infringement of the privileges of either House of Parliament.

386 Subsections (2) and (3) 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.

387 Subsection (4) explains the terms "client" and "communication" for the purposes of subsection (2) and (3).

388 Subsection (5) precludes the Commissioner from giving an assessment notice to a controller or processor with respect to the processing of personal data for journalistic, academic, artistic or literary purposes.

389 Subsection (6) lists other bodies to whom the Commissioner cannot give an assessment notice.

Section 148: Destroying or falsifying information and documents etc

390 This section provides that, where the Information Commissioner has given an information notice (see section 142) or an assessment notice (see section 146) requiring access to information, a document, equipment or other material, it is an offence to destroy or otherwise dispose of, conceal, block or (where relevant) falsify it, with the intention of preventing the Commissioner from viewing or being provided with or directed to it.

391 Subsection (3) provides that it is a defence for a person charged with this offence to prove that the destruction, disposal, concealment, blocking or falsification would have taken place in the absence of the notice being given to the person.

Section 149: Enforcement notices

392 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).

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

394 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.

395 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 of the GDPR; or has failed or is failing to comply with another provision of the GDPR – whether in their capacity as a certification provider or otherwise.

396 Subsection (5) enables the Commissioner to issue an enforcement notice against a controller for a failure to comply with regulations under section 137 in respect of charges payable to the Commissioner.

397 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.

398 Subsection (7) limits the requirements that the Commissioner may impose (which might include, but does not 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.

399 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 to comply with the data protection legislation not listed in this section.

400 Subsection (9) sets out in more detail the provision that regulations under this section can make.

Section 150: Enforcement notices: supplementary

401 This section sets out supplementary provisions in respect of enforcement notices given under section 149.

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

403 Subsection (3) explains that where the Commissioner gives an enforcement notice in reliance on section 149(2), the Commissioner's power under section 149(1)(b) includes power to suspend the data controller or processor from processing any personal data. Alternatively, the Commissioner can impose a ban in respect of a specified type of processing of personal data (by reference to the personal data involved, the purpose of the processing or the time at which the processing takes place).

404 Subsection (4) clarifies that the enforcement notice can establish the specific time or period within which the requirements set out in the enforcement notice must be complied with.

405 Subsection (5) requires an enforcement notice to provide information about rights under sections 162 and 164 (appeals etc) and the consequences of a failure to comply with it.

406 Subsection (6) prohibits an enforcement 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.

407 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.

408 Subsection (8) states that subsections (6) and (7) do not apply if the enforcement notice states why the requirements must be complied with urgently, but the Commissioner must not require the requirements to be complied with before the end of 24 hours from when the notice was issued.

409 Subsection (9) is self-explanatory.

Section 151: Enforcement notices: rectification and erasure of personal data etc

410 Subsection (1) makes it clear that this section 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 section also applies where a controller or processor has failed to comply with a data subject's rights to rectification, erasure or restriction of processing under Articles 16 to 18 of the GDPR or section 46, 47 or 100.

411 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 other data containing an expression of opinion 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.

412 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 that the data is inaccurate, or a statement of the true facts relating to the matters dealt with by the data.

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

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

Section 152: Enforcement notices: restrictions

415 This section 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.

416 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 section 174 that the processing was not wholly for such purposes, or the court has granted permission for the enforcement notice to be served.

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

418 Subsection (3) provides that an enforcement notice does not require a person to do something to the extent that requiring the person to do it would involve an infringement of the privileges of either House of Parliament.

Section 153: Enforcement notices: cancellation and variation

419 This section allows the Commissioner to cancel or amend an enforcement notice. It replicates the provisions enacted in section 41 of the 1998 Act.

420 Subsection (1) describes the way in which the Commissioner can cancel or amend an enforcement notice.

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

422 Subsection (3) sets out the circumstances in which an application under subsection (2) can be made.

Section 154: Powers of entry and inspection

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

Section 155: Penalty notices

424 This section gives the Commissioner a power to give a monetary penalty notice requiring a person to pay the Commissioner an amount determined by the Commissioner.

425 Subsection (1) sets out the circumstances in which the Commissioner can give a written penalty notice. 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 information notice, assessment notice or an enforcement notice.

426 Subsections (2) and (3) deal with the matters to which the Commissioner must have regard when considering deciding whether to give a penalty notice and when determining the amount of the penalty. By virtue of subsection (4), the duty to have regard to these matters does not apply where the fine relates to a failure to comply with regulations under section 137.

427 Subsection (5) introduces Schedule 16 which makes further provision about penalty notices.

428 Subsection (6) 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 to comply with the data protection legislation that are additional to those set out in subsection (1) and to make provision about the maximum amount of penalty (either the standard maximum amount or the higher maximum amount as described in section 157) that may be imposed for such failures.

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

Section 156: Penalty notices: restrictions

430 This section sets out the restrictions placed on the Commissioner in relation to the Commissioner's power to issue a penalty notice under section 155(1) in relation to different types of processing.

431 Subsections (1) and (2) replicate section 46 of the 1998 Act. Subsection (1) sets out the circumstances in which the Commissioner may give a penalty notice to a controller or processor with respect to the processing of personal data for the special purposes. Subsection (2) sets out the circumstances in which a court may grant leave for the notice to be given.

432 Subsection (3) prohibits the Commissioner from giving a penalty notice to a controller or processor with respect to the processing of personal data where the purposes and manner of the processing are determined by or on behalf of either House of Parliament.

433 Subsection (4) prohibits the Commissioner from issuing a penalty notice to the Crown Estate Commissioners or a person who is a controller by virtue of section 209(4).

Section 157: Maximum amount of penalty

434 This section makes provision about the maximum amount of fines that can be imposed for infringements of a provision of the GDPR, an infringement of a provision of Parts 3 or 4 or a failure to comply with an information notice, assessment notice or an enforcement notice.

435 Subsection (1) specifies the maximum penalty that can be issued by the Commissioner in relation to breaches of the GDPR with reference to Article 83 of the GDPR.

436 Subsection (2) specifies the maximum penalty amount in relation to breaches of Part 3 of the Act.

437 Subsection (3) specifies the maximum penalty amount in relation to breaches of Part 4 of the Act.

438 Subsection (4) specifies that the maximum penalty amount in relation to failure to comply with an information notice, assessment notice, or enforcement notice is the higher maximum amount (see subsection (5)).

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

440 Subsection (6) sets the standard maximum amount to be 10 million EUR or (in the case of an undertaking) 2% of the undertaking's total annual worldwide turnover, whichever is higher.

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

Section 158: Fixed penalties for non-compliance with charges regulations

442 This places an obligation on the Commissioner to publish a document specifying the penalty amounts for a failure to comply with regulations under section 137 (charges payable to the Commissioner by controllers). Different amounts may be specified for different types of failure.

443 Subsection (3) limits the maximum fine that can be issued for non-compliance to 150% of the highest charge payable pursuant to regulations made under section 137.

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

Section 159: Amount of penalties: supplementary

445 This section provides the Secretary of State with the power to introduce regulations for the purposes of Article 83 of the GDPR and section 157 which make provision that a person is or is not an undertaking or about how an undertaking's turnover is to be determined. The Regulations are subject to the affirmative resolution procedure.

Section 160: Guidance about regulatory action

446 Subsection (1) requires the Commissioner to produce and publish guidance about how she will exercise her functions in relation to assessment notices, enforcement notices, information notices and penalty notices. Subsection (2) enables the Commissioner to produce and publish guidance in respect of her other functions under Part 6.

447 Subsections (3) to (7) specify the matters which the guidance must include.

448 Subsection (8) allows the Commissioner to alter or replace the guidance.

449 Subsection (9) requires the Commissioner to consult the Secretary of State and such other persons as the Commissioner considers appropriate before publishing the guidance (including altered or replacement guidance).

450 Subsection (10) provides that the first guidance produced under this section is subject to the parliamentary approval procedure set out in section 161. Subsection (11) requires any subsequent guidance under this section to be laid before Parliament.

Section 161: Approval of first guidance about regulatory action

451 This section makes provision about the procedural requirements applying to the first guidance about regulatory action under section 160 and provides for that guidance to be subject to a process broadly equivalent to the negative resolution procedure.

Section 162: Rights of appeal

452 This section gives a person who is given a notice listed in subsection (1) a right to appeal against that notice.

453 Subsection (2) gives a person whose application for the cancellation or variation of an enforcement notice is refused a right to appeal against that refusal.

454 Subsection (3) gives a person a right to appeal against the amount specified in a penalty notice or a penalty variation notice whether or not the person appeals against the notice.

455 Subsection (4) gives a person right to appeal against a determination made under section 174.

Section 163: Determination of appeals

456 This section makes provision in relation to the determination of appeals under section 162 by the Upper Tribunal or the First-tier Tribunal.

457 In relation to appeals under section 162(2) or (4),

- subsection (2) empowers the tribunal to review any determination of fact on which the notice or decision against which the appeal is brought was based
- subsection (3) specifies the cases in which tribunal must allow an appeal or substitute another notice or decision
- subsection (4) requires the tribunal to dismiss the appeal in all other cases.

458 Subsection (5) provides in relation to an appeal against a refusal of an application for the cancellation or variation of the notice that the tribunal must cancel or vary the notice if the tribunal considers that there has been a change in circumstances.

459 Subsection (6) empowers the tribunal to cancel the Commissioner's determination where a person has appealed against the determination under section 162(4).

Section 164: Applications in respect of urgent notices

460 This section enables a person who is given an information notice, assessment notice or enforcement notice that requires the person to comply with it urgently to apply to the court to have the urgency statement set aside or for variation of the timetable for compliance. If the Commissioner has also asked the court to impose an information order under section 145 in respect of the information sought, it will be for the court to determine the most appropriate approach to be taken and might consider the two applications at the same time.

Section 165: Complaints by data subjects

461 This section 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 Articles 46 and 51 of the LED.

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

463 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.

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

465 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.

466 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.

467 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.

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

469 The provisions in this section 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 Act.

Section 166: Orders to progress complaints

470 This section 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 had 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.

471 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.

472 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.

473 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.

474 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 section 165(5).

Section 167: Compliance orders

475 This section 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 contained in 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 section does not apply to infringements of Part 4, as there are separate provisions in Part 4 enabling

data subjects to apply for court orders.

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

477 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.

478 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.

479 Subsection (4) confirms that a data subject can apply for a court order under this section 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.

480 Subsection (5) provides that where there are joint controllers under Part 3 whose responsibilities have been determined in accordance with the relevant provisions in Part 3, 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.

Section 168: Compensation for contravention of the GDPR

481 This section 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.

482 Subsections (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.

Section 169: Compensation for contravention of other data protection legislation

483 This section 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 section does not apply to compensation for a contravention of the GDPR, which is dealt with separately in section 168. As with section 168 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.

484 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.

485 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.

486 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.

487 Subsection (5) sets out the same definition of damage which applies to section 168, which includes distress. The inclusion of a definition of damage for the purpose of this section should not be taken to impact in any way on the meaning of "damage" in any other section in the Act.

Section 170: Unlawful obtaining etc of personal data

488 This section criminalises the deliberate or reckless obtaining, disclosing, procuring disclosure to another and retention of personal data without the consent of the data controller.

489 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.

490 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; for acting in the reasonable belief that they had a legal right or would have had the consent of the data controller; or was obtained for the special purposes, with a view to publication, and the obtaining of the data was reasonably believed to be justified as being in the public interest As worded, the section places a legal burden on the defendant to prove the relevant defences on the balance of probabilities.

491 Subsections (4) to (6) make it an offence to sell or offer to sell personal data that was obtained, disclosed or retained unlawfully.

Section 171: Re-identification of de-identified personal data

492 This section 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.

493 Subsection (1) sets out the elements of the offence.

494 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.

495 Subsection (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.

496 Subsection (4) provides further defences where the defendant can prove that: they reasonably believed that they had (or would have had) the consent of the data subjects to whom the information relates; they reasonably believed that they had (or would have had) the consent of the data controller responsible for de-identifying the information; or they acted for the special purposes, with a view to publication and the re-identification was reasonably believed to be justified as being in the public interest; or the effectiveness testing conditions as stated in section 172 (re-identification: effectiveness testing conditions) were met.

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

498 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.

499 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.

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

Section 172: Re-identification: effectiveness testing conditions

501 This section creates a specific defence for persons who re-identify information for the purposes of testing others' de-identification mechanisms. The section was developed to be of particular benefit to technology researchers.

502 Subsection (1) requires that both effectiveness testing conditions as provided for in subsections (2) and (3) are met in order for this defence to be relied upon.

503 The first condition, provided for in subsection (2), is that a person who re-identifies information acted with a view to testing the effectiveness of the de-identification system/s, acted without the intent to cause damage or distress, and acted in the reasonable belief that they were acting in the public interest.

504 The second condition, provided for in subsection (3), is that the person notified the Information Commissioner, or the controller(s) responsible for the de-identification, about their actions without undue delay and within 72 hours of the activity. Subsection (4) provides that (3) is satisfied by notifying at least one controller, where one or more controllers were responsible for the de-identification.

Section 173: Alteration etc of personal data to prevent disclosure to data subject

505 This section 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).

506 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.

507 Subsection (5) provides for defences for this offences where the defendant can prove that the alteration of the data would have occurred even if the subject access request had not been made, or that the defendant reasonably believed that the requester was not entitled to the information. As worded, the section places a legal burden on the defendant to prove the relevant defences on the balance of probabilities.

Section 174: The special purposes

508 This section defines "special purposes" as one or more of: the purposes of journalism, academic purposes, artistic purposes and literary 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. This section also defines "special purposes proceedings" as legal proceedings against a controller or processor relating (in whole or in part) to the processing of personal data processed for the special purposes.

509 Under this section, the Commissioner may make a written determination in relation to the processing of personal data for the special purposes that the data: is not being processed only for the special purposes, or is not being processed with a view to the publication of new material in relation to the special purposes. The Commissioner must provide written notice of any determination made to the controller and processor concerned. The section 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.

Section 175: Provision of assistance in special purposes proceedings

510 This section allows for individuals who are a party, or a prospective party, to special purposes related proceedings (as defined in section 174) 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 section also requires the Commissioner to notify the applicant as soon as reasonably practicable of a decision either way in respect of granting assistance.

511 If the Commissioner decides that the matter is not of substantial public importance, the section requires reasons to be given.

512 If the Commissioner decides that the matter is of substantial public importance, and therefore to grant assistance, the section requires the Commissioner to ensure that the person against whom the proceedings are brought 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 section 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.

513 This section 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.

Section 176: Staying special purposes proceedings

514 This section requires a court to stay, or in Scotland, sist, special purposes proceedings if the controller or processor claim, or it appears to the court, 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, academic, artistic, or literary 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 section also sets out the conditions under which the stay can be lifted.

Section 177: Guidance about how to seek redress against media organisations

515 This section requires the Commissioner to produce guidance about how individuals can seek redress where a media organisation (defined in subsection (2)) fails to comply with the data protection legislation, including guidance about making complaints and bringing claims before a court.

Section 178: Review of processing personal data for the purposes of journalism

516 This section requires the Commissioner to carry out a review of, and report on, the extent to which the processing of personal data for the purposes of journalism complied with the data protection legislation and good practice.

517 Subsection (2) sets the first review period to cover the first 4 years of the operation of the new data protection legislation (May 2018 to May 2022). Subsection (3) requires the review to start

within 6 months of this period ending and subsection (4) requires the review to conclude within 18 months of it starting. The Commissioner can therefore be expected to report by May 2024.

518 The review will then be repeated on a 5 year cycle. The second review period will cover the period May 2022 to May 2027.

519 Subsection (5) requires the review to cover all parts of the United Kingdom, including Northern Ireland.

520 Subsection (6) requires the Secretary of State to lay the Commissioner's report before Parliament, and send a copy of the report to the Scottish Ministers, the Welsh Ministers, and the Executive Office in Northern Ireland.

521 Subsection (7) gives effect to Schedule 17 which provides the Commissioner with further powers to conduct the review.

Section 179: Effectiveness of the media's dispute resolution procedures

522 This section requires the Secretary of State, every three years, to report on the use and effectiveness of alternative dispute resolution procedures designed to resolve complaints against media organisations in related to alleged breaches of data protection legislation.

523 Subsection (1) permits the Secretary of State to delegate the production of the report to an appropriate person.

524 Subsection (2) limits the scope of the report to alternative dispute resolution procedures provided by persons who produce codes of practice for relevant media organisations. Those codes will include, but is not limited to, the list of codes found in paragraph 26 of Schedule 2. Codes of practice directed at broadcasters are excluded from the scope of the report.

Section 180: Jurisdiction

525 This section sets out which courts have jurisdiction for specified provisions in the Act. 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.

526 Subsection (2) sets out the relevant provisions of the Act and the GDPR to which the jurisdiction provision in subsection (1) applies.

527 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).

528 Information orders under section 145 can normally be made by the High Court or county court or, in Scotland, by the Court of Session or the sheriff. Subsection (4) makes an exception for cases in which the information notice contains an urgency statement, when only the High Court or, in Scotland, the Court of Session can make an information order.

529 Subsection (5) provides that applications to challenge urgent notices under section 164 are to be dealt with by the High Court or, in Scotland, by the Court of Session.

Section 181: Interpretation of Part 6

530 This section provides an interpretation of certain terms used in Part 6 of the Act.

Part 7: Supplementary and final provision

Section 182: Regulations and consultation

531 This section makes provision concerning the form, process and procedure for making regulations under the powers in the Act, including consultation requirements. It makes it clear that, before making regulations, the Secretary of State must consult the Information Commissioner and such other persons as he considers appropriate, save for some exceptions. Those other persons will depend on the nature of the regulations in question, but an illustrative example would be where the regulations touch on healthcare matters and/or the processing of patient data. In such a case, the Secretary of State might consider it appropriate to consult, for example, the National Data Guardian for Health and Care, relevant healthcare bodies and relevant medical associations.

Section 183: Power to reflect changes to the Data Protection Convention

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

533 Subsection (4) limits that regulation making power in subsection (1) to a period of three years from the date of Royal Assent (of this Act).

Section 184: Prohibition of requirement to produce relevant records

534 This section 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.

535 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 section places a legal burden on the defendant to prove the relevant defence on the balance of probabilities.

536 Subsection (5) expands on 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.

537 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 18.

538 This section is similar to section 56 of the 1998 Act, but the list of relevant records in Schedule 18 is wider because it now includes medical records.

Section 185: Avoidance of certain contractual terms relating to health records

539 This section 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.

540 Subsection (4) sets out the meanings of the terms "data subject access rights" as it applies in this section.

Section 186: Data subject's rights and other prohibitions and restrictions

541 This Act gives data subject rights and data controller obligations special status. This section 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 Act.

Section 187: Representation of data subjects with their authority

542 This section 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 rights to bring judicial review proceedings against the Commissioner and to apply for a tribunal order against the Commissioner under section 166, 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 section reflects the rights in 80(1) of the GDPR and Article 55 of the LED.

543 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.

544 Subsection (2) sets out, in relation to the data protection legislation other than the GDPR, 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.

545 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.

546 Subsection (5) explains that references to a "representative body" in this Act are to a body or organisation which is authorised to exercise a right on behalf of a data subject.

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

Section 188: Representation of data subjects with their authority: collective proceedings

548 This section provides the Secretary of State with the power to make regulations enabling representative bodies to bring collective proceedings on behalf of data subjects in England and Wales or Northern Ireland by combining two or more claims in respect of data subjects' rights, where those data subjects have given their authorisation to the representative body.

Section 189: Duty to review provision for representation of data subjects

549 This section imposes a duty on the Secretary of State to review the operation of the provisions in the GDPR and in section 187 of the Act which enable a representative body to exercise data subjects' rights with their authority. The review will also consider the merits of enabling a representative body to exercise data subjects' rights under the GDPR to complain to the Information Commissioner, to seek judicial remedies, or to seek compensation, without being authorised to do so by data subjects, as well as the merits of enabling children's rights organisations to represent children. The Secretary of State is required to lay a report of the review before Parliament within 30 months of the commencement of section 187

550 Subsection (4) requires the Secretary of State to consider and analyse specified matters relating to children. Subsection (5) requires certain persons to be consulted before preparing the report.

Section 190: Post-review powers to make provision about representation of data subjects

551 This section provides the Secretary of State with the power to enable representative bodies to exercise certain rights of data subjects under the GDPR on their behalf, without their authorisation, following the review provided for by section 189.

Section 191: Framework for Data Processing by Government

552 This section makes provision for the Secretary of State to issue statutory guidance (a "Framework for Data Processing by Government") about the processing of personal data in connection with the exercise of functions of the persons or bodies listed in subsection (1). Any person carrying out such processing must have regard to this guidance. The Secretary of State may by regulations specify additional persons with functions of a public nature who are required to have regard to the Framework.

553 Subsection (3) provides that the guidance will not apply to the devolved administrations.

554 Subsection (5) requires the Secretary of State to consult the Commissioner and any other person the Secretary of State considers appropriate when preparing a guidance document, or amendments to a document, issued under this section.

555 Subsection (6) provides that regulations made under subsection (1) are subject to the negative resolution procedure.

Section 192: Approval of the Framework

556 This section establishes that, before it can be issued, the Framework must be subject to Parliamentary scrutiny through a process broadly equivalent to the negative resolution procedure.

Section 193: Publication and review of the Framework

557 This section requires the Secretary of State to publish the Framework and any subsequent amendments to the Framework or replacements. It also requires the Secretary of State to keep the Framework under review and to update it as appropriate.

Section 194: Effect of the Framework

558 This section provides that persons undertaking relevant processing of personal data must have regard to the Framework but are not liable to legal proceedings solely because of a failure to act in accordance with it.

559 Subsection (3) provides that the Framework is admissible in evidence in legal proceedings.

560 Subsection (4) establishes that the Framework must, where relevant, be taken into account by a court or tribunal.

561 Subsection (5) provides that the Commissioner must take the Framework into account if she considers it relevant to a question arising in connection with her functions. For example, if the Commissioner were to be investigating a data breach by a Government department she may consider it relevant to consider whether or not that department had applied the principles set out in the Framework. The Commissioner remains free to disregard the Framework wherever she considers it irrelevant.

562 More generally, the Commissioner remains free to disagree with the Framework's contents and to include whatever she sees fit in her own Code.

Section 195: Reserve forces: data sharing by HMRC

563 This section provides for HMRC to supply the Secretary of State with the contact details of members of the ex-regular reserve force and former members of the armed forces so that they may be contacted regarding their liability to be called out or recalled for service under the Reserved Forces Act 1996. The details supplied may also be used for defence purposes connected with their service in the forces (whether past, present or future). It is an offence for the details supplied to be disclosed without the consent of the Commissioners for Revenue and Customs.

Section 196: Penalties for offences

564 This section sets out the penalties for the offences in this Act.

565 Subsection (1) sets out the penalties for the summary only offences in sections 119 (inspection of personal data in accordance with international obligations), 173 (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.

566 Subsection (2) sets out the maximum penalties for offences that can be tried summarily or on indictment. These include offences in sections 132 (confidentiality of information), 144 (false statements made in response to information notices), 148 (destroying or falsifying information and documents etc), 170 (unlawful obtaining etc of personal data), 171 (re-identification of de-identified personal data) and 184 (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.

567 Subsection (4) provides a power for the court to order the forfeiture and destruction of material obtained under offences in sections 170 and 184.

568 Subsection (5) provides any individual (other than the offender) with an interest in the data the right to demonstrate to the court why it should not forfeit or destroy such material.

Section 197: Prosecution

569 This section makes it clear which enforcement agencies are responsible for prosecuting offences under this Act. 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 section for Scotland as for other parts of the UK.

570 Subsections (3) to (7) concern periods allowed for commencement of prosecutions for an offence under section 173 of this Act (alteration etc. of personal data to prevent disclosure).

Section 198: Liability of directors etc

571 This section 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. The provision in this section substantively replicates section 61 of the 1998 Act.

Section 199: Recordable offences

572 This section allows for the National Police Records (Recordable Offences) Regulations 2000

(S.I. 2000/1139) to be read as making offences under this Act recordable. Offenders who are arrested for a recordable offence may have their fingerprints and DNA samples taken, and their convictions will be recorded on the Police National Computer.

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

Section 200: Guidance about PACE codes of practice

574 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).

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

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

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

Section 201: Disclosure of information to the Tribunal

578 This section 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.

Section 202: Proceedings in the First-tier Tribunal: contempt

579 This section 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.

580 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.

581 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 had been committed in relation to the Upper Tribunal.

582 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.

583 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 section the First-tier Tribunal will now certify the offence to the Upper Tribunal.

Section 203: Tribunal Procedure Rules

584 This section 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 Act) are exercised. It also allows Tribunal Procedure Rules to be made about the exercise of a data subject's rights to apply for an order against the Commissioner under section 166 of this Act, including the exercise of those rights by a representative body.

585 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.

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

Section 204: Meaning of "health professional" and "social work professional"

587 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. Section 10(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.). Section 11(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 responsibility of, a "health professional" or a "social work professional". Under paragraph 3 of Schedule 1 to this Act, processing in the public interest for public health purposes may only be carried out in certain specified circumstances, including by, or under the responsibility of a "health professional".

588 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.

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

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

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

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

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

Section 205: General interpretation

594 This section is self-explanatory in defining terminology used in this Act.

595 "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.

596 Subsection (2) clarifies that (contrary to their usual interpretation in UK law) periods of time referred to in this Act are generally to be interpreted in accordance with Article 3 of EC Regulation 1182/71, which makes provision about the calculation of periods of hours, days, weeks, months and years. Where a period is expressed in days, weeks, months or years and is calculated from the moment at which an event occurs, the day during which the event occurs is not included within the period i.e. the clock starts running on the following day. Where a period is expressed in hours and is calculated from the moment at which an event occurs the hour during which the event occurs is not included within the period i.e. the clock starts

running from the following hour. Subsection (2) also provides a list of exceptions to this general interpretation provision – for example, for parliamentary processes, where the usual rules on time periods will instead apply.

Section 206: Index of defined expressions

597 This section lists certain terms defined in the Act and signposts where the definition may be found.

Section 207: Territorial application of this Act

598 This section provides details of the territorial application of the Act. 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.

599 Subsection (2) provides that the Act applies to processing in the context of the activities of an establishment of a controller or processor in the UK. This is similar to Article 3(1) of the GDPR. It applies to all regimes under the Act.

600 Subsection (3) provides that, in certain circumstances, the Act also applies to processing to which the GDPR applies which is carried out in the context of activities of an establishment of a controller or processor in a country or territory that is not part of the EU. This is similar to Article 3(2) of the GDPR. Subsection (3) does not apply for the applied GDPR or for Parts 3 or 4 of the Act.

601 This section also defines a "person who has an establishment 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, or a person who maintains in the UK an office, branch or agency through which they carry out an activities or other stable arrangements.

Section 208: Children in Scotland

602 This section applies to Scotland. It provides that a child under 16 can exercise their rights or give consent under the data protection legislation if the child 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.

603 This section is to be read in conjunction with Article 8 of the GDPR. Article 8, read with section 9 of this Act, 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.

Section 209: Application to the Crown

604 The GDPR does not contain any provision to exempt the Crown from its requirements. Likewise, section 63 of the 1998 Act bound the Crown. This section makes similar, and related, provision. For example, where crown bodies enter into controller-processor relationships with each other, subsection (3) provides that that arrangement may be governed by a Memorandum of Understanding rather than a contract (see Article 28(3) of the GDPR).

Section 210: Application to Parliament

605 The GDPR does not contain any provision to exempt Parliament from its requirements. Likewise, section 63A of the 1998 Act applied that Act to the processing of personal data by or on behalf of either House of Parliament. This section makes similar provision in respect of this Act, save in relation to Parts 3 and 4.

Section 211: Minor and consequential provision

606 This section provides for minor and consequential amendments to other legislation, which follow as a consequence of the GDPR and this Act. The minor and consequential amendments are contained in Schedule 19 and include the repeal of the 1998 Act. The section confers on the Secretary of State a regulation-making power to make further consequential amendments, which arise from this Act. 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 under this section are subject to the negative procedure.

Section 212: Commencement

607 This section provides the Secretary of State with a power to make regulations bringing the Act into force, including making different provision for different areas. Certain provisions listed in subsection (2) come into force on the date of Royal Assent. Other provisions listed in subsection (3) come into force at the end of the period of 2 months beginning on the date of Royal Assent.

Section 213: Transitional provision

608 This section gives effect to Schedule 20 which makes necessary transitional provision.

609 Subsection (2) provides 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 Act.

Section 214: Extent

610 This section is self-explanatory.

Section 215: Short title

611 This section is self-explanatory.

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

612 This Schedule specifies the conditions and associated safeguards that must be met in order for special categories of data to be processed pursuant to section 10.

613 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.

614 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.

615 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.

616 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 paragraph 35 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 and research etc

617 Paragraph 1 relates to Article 9(2)(b) of the GDPR and allows the processing of special categories of data in in connection with employment, social security and social protection where obligations or rights are imposed or conferred by law on the controller or the data subject. The section would cover a wide range of social services' interventions as Article 2(b) of Regulation (EU) 458/2007 covers interventions which are needed to support people who may be suffering difficulties in relation to health care or sickness; disability; old age; survivorship; family and children; unemployment; housing; and social exclusion. This condition is only met if the controller has an appropriate policy document in place (as defined in Part 4).

618 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 section 11(1), which defines circumstances that are included in the Article 9(3) requirement.

619 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 responsibility of, a health professional, or by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

620 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 section 19) and is in the public interest.

Part 2 – Substantial public interest conditions

621 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 Act.

622 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.

623 Paragraph 6 permits processing of special categories of data that is in the substantial public interest and is necessary for the exercise of a function conferred on a person by an enactment or rule of law; or the exercise of a function of the Crown, a Minister of the Crown or a Government department.

624 Paragraph 7 permits processing that is necessary for the administration of justice or for the exercise of a function of either House of Parliament.

625 Paragraph 8 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.

626 Paragraph 9 permits processing of special categories of data necessary for the purposes of promoting or maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in organisations where the processing can reasonably be carried out without the consent of the data subject and the processing does not cause substantial damage or substantial distress to an individual.

627 Paragraph 10 permits processing of special categories of data for the purposes of the prevention or detection of any unlawful act where it is necessary for reasons of substantial public interest or where seeking the consent of the data subject to the processing would prejudice those purposes, which would cover a situation where giving the data subject a choice or giving them the necessary information required for valid consent would prejudice the purpose, or where valid consent is not possible because a refusal to consent could cause detriment.

628 Paragraph 11 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 the processing is necessary for reasons of substantial public interest and seeking the consent of the data subject would prejudice those purposes, which would cover a situation where giving the data subject a choice or giving them the necessary information required for valid consent would prejudice the purpose, or where valid consent is not possible because a refusal to consent could cause detriment.

629 Paragraph 12 permits processing of special categories of data for the purposes of complying with, or assisting others to comply with, a regulatory requirement relating to unlawful acts, dishonesty etc. This paragraph allows private companies (in particular in the financial services sector) to process special categories of personal data where necessary to screen against UK laws such as the Proceeds of Crime Act 2002 to help financial institutions identify customers suspected of money laundering, and this paragraph further permits processing to screen against other regulatory requirements including widely-recognised sectoral guidelines such as those promulgated by the Financial Action Task Force. Additional requirements are that the controller cannot reasonably be expected to obtain the consent of the data subject to the processing and the processing is necessary for reasons of substantial public interest.

630 Paragraph 13 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.

631 Paragraph 14 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.

632 Paragraph 15 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).

633 Paragraph 16 permits processing of special categories of data by a not-for-profit body which provides support to individuals with a particular disability or medical condition, for the purpose of raising awareness of the disability or medical condition, or assisting those affected by it. This includes the work undertaken by patient support groups. These are groups who provide services to those suffering from (typically rare) diseases or other medical conditions. Additional requirements are that the processing can reasonably be carried out without the consent of the data subject and that it is necessary for reasons of substantial public interest.

634 Paragraph 17 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).

635 Paragraph 18 permits processing of special categories of data required for the protection of children or of adults at risk. This makes is clear that front-line practitioners and others can lawfully process personal data by retaining records and sharing information where necessary, for the purpose of safeguarding children and vulnerable adults. The processing must be necessary for reasons of substantial public interest and must be carried out without the consent of the data subject for one of the specified reasons.

636 Paragraph 19 permits processing of special categories of data which is necessary to protect the economic well-being of adults who are less able to protect their own economic well-being by reason of a physical or mental injury, illness or disability where the processing is necessary for reasons of substantial public interest and is carried out without the consent of the data subject for one of the specified reasons.

637 Paragraph 20 permits processing of data concerning health, or data revealing racial or ethnic origin, religious or philosophical beliefs or trade union membership, or genetic data where it is necessary for an insurance purpose and is necessary for reasons of substantial public interest.

638 Sub-paragraphs (2), (3) and (4) provide specific safeguards for those data subjects who: (i) do not have rights or obligations in connection with the insurance contract or the insured person, and (ii) where the processing is not carried out for the purpose of measures or decisions with respect to them. For example, a witness to an event giving rise to an insurance claim or a sibling of a person seeking health insurance might fall into this category. Processing of data relating to these data subjects is only permitted if the data controller cannot reasonably be expected to obtain the consent of the data subject and they are not aware of the data subject withholding their consent.

639 "Insurance purpose" is defined in sub-paragraph (5). The definition includes: processing necessary for advising on, arranging, underwriting or administering an insurance contract and processing necessary for administering a claim under an insurance contract or against the Motor Insurers' Bureau. Processing necessary for exercising a right or obligation arising under an enactment or rule of law, such as subrogated rights, is also included. Sub-paragraph (6) further clarifies the definition of "insurance contract".

640 Paragraph 21 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.

641 Paragraph 22 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, fundraising, 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.

642 Paragraph 23 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).

643 Paragraph 24 permits the disclosure of special categories of data to an elected representative or a person acting with the authority of such a representative and in response to a communication to the controller from that representative or person which was made in response to a request from an individual. The disclosure must be necessary for the purpose of responding to the subject matter of the communication, the personal data must be relevant to the subject matter of the communication, and the processing must be carried out without the data subject's consent for one of the reasons specified in sub-paragraph (2).

644 Paragraph 25 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, a member of the National Assembly for Wales 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.

645 Paragraph 26 allows the processing of special categories of data where the processing consists of the publication of a judgment or other decision of a court or tribunal, or is necessary for the purposes of publishing such a judgment or decision.

646 Paragraph 27 permits bodies who are responsible for monitoring or eliminating doping in a sport or sporting event, to undertake processing of special categories of data necessary for those purposes.

647 Paragraph 28 permits processing that is necessary for the purposes of measures designed to protect the integrity of a sport or sporting event. Sub-paragraph (2) lists the behaviours and activities which this condition is attempting to protect against in sport or sporting events. These include: dishonesty, malpractice or other seriously improper conduct, or a failure by a person participating in the sport or event in any capacity to comply with standards of behaviour set by a body or association with responsibility for the sport or sporting event. The processing must be in the substantial public interest. It must also be necessary to carry out the processing without the consent of the data subject so as not to prejudice the purposes designed to protect the integrity of a sport or sporting event, which would cover a situation where giving the data subject a choice or giving them the necessary information required for valid consent would prejudice the purpose, or where valid consent is not possible because a refusal to consent could cause detriment.

Part 3 – Additional conditions relating to criminal convictions etc

648 This part relates the processing of personal data relating to criminal convictions and offences or related security measures under Article 10 of the GDPR.

649 Paragraph 29 permits processing of personal data relating to criminal convictions etc. if the data subject has given his or her consent.

650 Paragraph 30 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.

651 Paragraph 31 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.

652 Paragraph 32 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.

653 Paragraph 33 permits processing of personal data relating to criminal convictions etc. necessary for the purpose of legal proceedings; obtaining legal advice; or establishing, exercising or defending legal rights.

654 Paragraph 34 permits processing of personal data relating to criminal convictions etc. necessary when a court or tribunal is acting in its judicial capacity.

655 Paragraph 35 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, where the controller has an appropriate policy document in place.

656 Section 10(4) and (5) have the effect that processing of criminal convictions etc. data is also permitted under certain conditions in Parts 1 and 2 of the Schedule where the special categories of data permitted to be processed are not limited. Since there is no requirement for processing under Article 10 of the GDPR to be in the substantial public interest, paragraph 36(1) disapplies this express requirement where it exists in Part 2 for the purposes of processing criminal convictions etc. data.

657 Paragraph 37 extends paragraph 20 of Schedule 1 so that the processing of criminal conviction etc. data is permitted for an insurance purpose. Because paragraph 20 only permits the processing of specified special categories of data, this provision is needed to ensure that criminal conviction etc. data can be processed.

Part 4 – Appropriate policy document and additional safeguards

658 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 paragraph 35 of Schedule 1 and apply in addition to any express safeguards that are required under any specific processing condition.

659 Paragraph 39 defines the safeguard that "the controller has 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.

660 Paragraph 40(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.

661 Paragraph 40(2) defines the "relevant period" for the purposes of paragraph 40(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 beginning when the controller ceases to carry out such processing.

662 Paragraph 41 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 paragraph 35 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)

663 Paragraph 1 sets out the GDPR provisions restricted or adapted by the exemptions in this Part, the "listed GDPR provisions".

664 Paragraph 2 restricts the application of the listed GDPR provisions and Article 34(1) and (4) of the GDPR (communication of personal data breach to the data subject) 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.

665 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.

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

667 Paragraph 4 restricts the application of the certain GDPR provisions to personal data processed for the purposes of the maintenance of effective immigration control, or the investigation or detection of activities that would undermine the maintenance of effective immigration control, to the extent that the application of those provisions would be likely to prejudice those purposes. Sub-paragraphs (3) and (4) make provision relating to the further processing of personal data for the immigration purposes. For the purposes of paragraph 4 a narrower set of listed GDPR provisions applies as set out in sub-paragraph (2).

668 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.

669 Paragraph 5(2) and (3) restrict the listed GDPR provisions where the disclosure of personal information is required by law or necessary for the purposes of or in connection with legal proceedings or necessary for obtaining legal advice or establishing exercising or defending legal rights. They replicate the exemptions under section 35 of the 1998 Act.

Part 2 – Restrictions based on Article 23(1): restrictions of rules in Articles 13 to 21 and 34

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

671 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.

672 Paragraph 8 restricts the application of the listed GDPR provisions to personal data processed for the purposes of discharging statutory audit functions.

673 Paragraph 9 restricts the application of the listed GDPR provisions to personal data processed for the purposes of discharging specified functions of the Bank of England.

674 Paragraph 10 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.

675 Paragraph 11 restricts the application of the listed GDPR provisions to personal data processed by certain other public bodies for the purposes of discharging their statutory functions, as specified in the table.

676 The restrictions in paragraphs 7, 8, 9, 10 and 11 apply to the extent that the processing would be likely to prejudice the proper discharge of those functions. They replace provision under section 31 of the 1998 Act.

677 Paragraph 13 restricts the application of the listed GDPR provisions and Article 34(1) and (4) of the GDPR (communication of personal data breach to the data subject) to personal data processed for the purposes of avoiding an infringement of parliamentary privilege. This replicates section 35A of the 1998 Act.

678 Paragraph 14(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.

679 Paragraph 14(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.

680 Paragraph 14(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.

681 Paragraph 15 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 – Restriction based on Article 23(1): protection of rights of others

682 Paragraphs 16 and 17 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

683 Paragraph 18 sets out the listed GDPR provisions restricted by the exemptions in this Part.

684 Paragraph 19 restricts the application of the listed GDPR provisions to personal data that consists of information over which a claim to legal professional privilege (or in Scotland, confidentiality in communications) could be maintained in legal proceedings, or information covered by a duty of confidentiality owed by a professional legal adviser to a client of the adviser. It expands on the exemption in paragraph 10 of Schedule 7 to the 1998 Act.

685 Paragraph 20 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 Act. This replicates the exemption in paragraph 11 of Schedule 7 to the 1998 Act.

686 Paragraph 21 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 (S.I. 2000/184).

687 Paragraph 22 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.

688 Paragraph 23 restricts the application of the listed GDPR 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.

689 Paragraph 24 restricts the application of the listed GDPR provisions to personal data consisting of a reference given (or to be given) in confidence, for example for education or employment purposes. This replicates and extends the exemption in paragraph 1 of Schedule 7 to the 1998 Act.

690 Paragraph 25 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

691 This Part provides that the GDPR provisions listed in paragraph 26(8) will not apply when personal data is being processed with a view to publication for one or more of the special purposes (as defined in paragraph 26(1)), the controller reasonably believes that the publication would be in the public interest and that the application of any of the listed GDPR provisions would be incompatible with the special purposes.

692 Paragraphs 26(4) to (6) set out the matters 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 26(6).

693 Paragraph 26(7) allows the Secretary, by regulations subject to the affirmative resolution procedure, to amend the list of specified codes of practice listed in paragraph 26(6).

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

694 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.

695 Paragraph 27 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 section 19, and the results of research or any resulting statistics are not made available in a form which identifies the data subject.

696 Paragraph 28 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 section 19.

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

697 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 (S.I. 2000/413);
- The Data Protection (Subject Access Modification) (Education) Order 2000 (S.I. 2000/414); and
- The Data Protection (Subject Access Modification) (Social Work) Order 2000 (S.I. 2000/415).

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

699 Part 2 restricts the application of the listed GDPR provisions in relation to data concerning health. 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;
- 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.

700 Part 3 restricts the application of the listed GDPR provisions in relation to social work data. 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;
- a request is made on behalf of the data subject for information the data subject has expressly indicated should not be disclosed.

701 Part 4 restricts the application of the listed GDPR provisions in relation to education data. 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.

702 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

703 This Schedule seeks to preserve to the substance of the Data Protection (Miscellaneous Subject Access Exemptions) Order 2000 (S.I. 2000/419).

704 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.

705 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

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

707 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.

708 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.

709 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.

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

711 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

712 As set out in Article 2(2), the GDPR only applies to the processing of data in the course of an activity which is subject to Union law. Chapter 3 of Part 2 of this Act provides for a separate regime to apply GDPR standards to general processing in the UK which is outside the scope of the GDPR. This Schedule specifies how the GDPR standards will be applied to areas outside the scope of Union law. This Schedule makes the necessary modifications to the provisions to reflect the application to non-Union law activities, creating an applied GDPR and applied Chapter 2 of Part 2. These provisions describe how Union law references should be interpreted in the domestic context.

713 In Part 1 of Schedule 6, paragraphs 2 to 6 make general modifications to terms used throughout the GDPR. Paragraphs 7 onwards make more specific provision on an article-by-article basis, for example to remove provision which is irrelevant in a UK-only context. A given article of the GDPR may therefore be modified for the purposes of the applied GDPR by multiple paragraphs contained in this Schedule. In a similar vein, Part 2 of the Schedule concerns the application of Chapter 2 of Part 2 of the Act to general processing in the UK which is outside the scope of the GDPR.

714 More specifically, paragraph 2 explains that save as otherwise specified, references in this Schedule to "this Regulation" and to provisions of the GDPR, refer to the applied GDPR.

715 Paragraph 3 specifies that 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(3) explains the meaning of "domestic law".

716 Paragraph 4 specifies that references to "the Union", a "member state" and "member states" should be regarded as meaning the United Kingdom unless otherwise specified.

717 Paragraph 5 specifies that references to a "supervisory authority", a "competent supervisory authority" or "supervisory authorities" should be regarded as meaning the Information Commissioner save as otherwise specified.

718 Paragraph 6 specifies that references to "the national parliament" should be read as references to both Houses of Parliament.

719 Paragraph 7 provides for the material scope of the applied GDPR – i.e. processing falling within Chapter 3 of Part 2 of the Act.

720 Paragraph 8 specifies that the territorial application of the applied GDPR is the same as the territorial application of the Act, save for minor changes.

721 Paragraph 9 modifies Article 4 of the GDPR (definitions) for the applied GDPR to make clear,

for example, that references to "Commissioner" should be regarded as meaning the Information Commissioner.

722 Paragraph 10 modifies Article 6 of the GDPR (lawfulness of processing) for the applied GDPR, to insert a cross-reference to the power in the Act to make further provision in secondary legislation.

723 Paragraph 11 modifies Article 8 of the GDPR (conditions applicable to child's consent in relation to information society services) for the applied GDPR to make clear that the conditions are subject to this Act and that domestic contract law applies, rather than the "general contract law of Member States".

724 Paragraph 12 modifies Article 9 of the GDPR (processing special categories of personal data) for the applied GDPR to replace references to "Union or Member State law" and other terms with domestic equivalents.

725 Paragraph 13 modifies Article 10 of the GDPR (processing of personal data relating to criminal convictions and offences) for the applied GDPR to make clear that the relevant safeguards are found in domestic law, rather than Union or Member State law.

726 Paragraph 14 modifies Article 12 of the GDPR (transparent information etc for the exercise of the rights of the data subject) for the applied GDPR to omit paragraph 8 (ability of the European Commission to provide for standardised icons).

727 Paragraph 15 modifies Article 13 of the GDPR (personal data collected from data subject: information to be provided) for the applied GDPR to omit the reference to the "controller's representative" and insert a cross-reference to Article 45(3) of the GDPR (transfers on the basis of an adequacy decision).

728 Paragraph 16 modifies Article 14 of the GDPR (personal data collected other than from data subject: information to be provided) for the applied GDPR to omit the reference to the "controller's representative", insert a cross-reference to Article 45(3) of the GDPR (transfers on the basis of an adequacy decision) and make clear that the relevant applicable law for Article 14(5)(c) is domestic law.

729 Paragraph 17 modifies Article 17 of the GDPR (right to erasure) for the applied GDPR to replace references to "Union or Member State law" with references to domestic law.

730 Paragraph 18 modifies Article 18 of the GDPR (right to restriction of processing) for the applied GDPR to replace the reference to the "reasons of important public interest of the Union or of a Member State" to refer instead to the United Kingdom.

731 Paragraph 19 omits the reference to Directive 2002/58/EC (the Privacy and Electronic Communications Directive) in Article 21 of the GDPR (right to object) for the applied GDPR.

732 Paragraph 20 modifies Article 22 of the GDPR (automated individual decision-making, including profiling) for the applied GDPR to use the definition of "qualifying significant decision" provided for in section 14 of the Act.

733 Paragraph 21 modifies Article 23 of the GDPR (restrictions) for the applied GDPR to omit a reference to the "Union or Member State law to which the data controller or processor is subject" and replace it with a reference to section 15 of, and Schedules 2, 3 and 4 to, the Act, and to make clear that the reference to "of the Union or of a Member State" means the "United Kingdom".

734 Paragraph 22 modifies Article 26 of the GDPR (joint controllers) for the applied GDPR to replace references to "Union or Member State law to which controllers are subject" to refer to

domestic law.

735 Paragraph 23 omits Article 27 of the GDPR (representatives of controllers or processors not established in the Union) from the applied GDPR.

736 Paragraph 24 modifies Article 28 of the GDPR (processor) for the applied GDPR to replace references to Union or Member State law with reference to domestic law, and to omit paragraph 7 (ability of the European Commission to lay down standard contractual clauses).

737 Paragraph 25 modifies Article 30 of the GDPR (records of processing activities) for the applied GDPR to omit references to the "controller's representative" and "processor's representative" and to add cross-references to section 28 of the Act.

738 Paragraph 26 modifies Article 31 of the GDPR (cooperation with the supervisory authority) for the applied GDPR to omit reference to controllers' and processors' representatives.

739 Paragraph 27, in relation to Article 35 of the GDPR (data protection impact assessment), omits from the applied GDPR the requirements on the Information Commissioner found in paragraphs 4, 5, 6 and 10 of that Article in relation to cross-border consistency.

740 Paragraph 28 modifies paragraph 4 of Article 36 of the GDPR (prior consultation) for the applied GDPR to make clear that it is for the "Secretary of State" rather than the "Member State" to undertake relevant consultation, and to omit paragraph 5 (ability of Member State law to make further provision).

741 Paragraph 29 modifies Article 37 of the GDPR (designation of the data protection officer) for the applied GDPR to omit paragraph 4 (ability of Member State law to make further provision, etc).

742 Paragraph 30 modifies Article 39(1) of the GDPR (tasks of the data protection officer) for the applied GDPR to replace references to "other Union or Member State data protection provisions" with references to "other rules of domestic law relating to data protection".

743 Paragraph 31 modifies Article 40 of the GDPR (codes of conduct) for the applied GDPR to omit paragraphs 3 (application to controllers not subject to the Regulation) and 7 to 11 (application to cross-border processing activities), and to make clear that it is for the Commissioner to encourage the drawing up of codes of conduct, rather than "the Member States, the supervisory authorities, the Board and the [European] Commission".

744 Paragraph 32 modifies Article 41 of the GDPR (monitoring of approved codes of conduct) for the applied GDPR to omit paragraph 3 (cross-border consistency).

745 Paragraph 33 modifies Article 42 of the GDPR (certification) for the applied GDPR to omit paragraph 2 (application to controllers not subject to the Regulation) and paragraph 8 (cross-border consistency), and to make clear that it is for the Commissioner to encourage the establishment of data protection certification mechanisms and of data protection seals and marks, rather than "the Member States, the supervisory authorities, the Board and the [European] Commission".

746 Paragraph 34 modifies Article 43 of the GDPR (certification bodies) for the applied GDPR to omit provision relating to cross-border consistency. It also omits paragraph 8 (ability of the European Commission to adopt delegated or implementing acts in relation to certification mechanisms).

747 Paragraph 35 modifies Article 45 of the GDPR (transfers on the basis of an adequacy decision) for the applied GDPR to make clear that relevant decisions are decisions made by the European Commission in accordance with Article 45 of the GDPR, rather than a separate

process.

748 Paragraph 36 modifies Article 46 of the GDPR (transfers subject to appropriate safeguards) for the applied GDPR to omit paragraph 2(c) (ability of the European Commission to lay down standard contractual clauses) and the second half of 2(d) (requirement for the European Commission to approve standard data protection clauses). It also omits paragraph 4 (cross-border consistency).

749 Paragraph 37 modifies Article 47 of the GDPR (binding corporate rules) to omit provision relating to cross-border consistency and to replace references to "the competent courts of the Member States" and "on the territory of a Member State" with references to "a court" and "United Kingdom" respectively.

750 Paragraph 38 modifies Article 49 of the GDPR (derogations for specific situations) for the applied GDPR to make clear that an adequacy decision is a decision under Article 45(3) of the GDPR; replace references to "Union law or in the law of the Member State to which the controller is subject" with references to "domestic law" and clarify that paragraph 1 is subject to domestic law, through section 18(2) of this Act.

751 Paragraph 39 modifies Article 50 of the GDPR (international co-operation for the protection of personal data) for the applied GDPR to omit reference to obligations being placed on the Commission.

752 Paragraph 40 modifies Article 51 of the GDPR (supervisory authority) for the applied GDPR to replace references to a supervisory authority with specific references to the Commissioner. It also omits paragraphs 2 to 4 (cross-border consistency), and the requirement on the Commissioner to facilitate the free flow of personal data covered by the applied GDPR "within the Union".

753 Paragraph 41 modifies Article 52 of the GDPR (independence) for the applied GDPR to replace references to a supervisory authority with specific references to the Commissioner. It also omits paragraphs 4 to 6 (obligations on Member States).

754 Paragraph 42 omits Article 53 of the GDPR (general conditions for the members of the supervisory authority) from the applied GDPR.

755 Paragraph 43 omits Article 54 of the GDPR (rules on the establishment of the supervisory authority) from the applied GDPR.

756 Paragraph 44 modifies Article 55 of the GDPR (competence) for the applied GDPR to omit references to competence in relation to cross-border processing activities.

757 Paragraph 45 omits Article 56 of the GDPR (competence of the lead supervisory authority) from the applied GDPR.

758 Paragraph 46 modifies Article 57 of the GDPR (tasks) for the applied GDPR to remove references to cross-border processing activities and the need for cross-border consistency. It also introduces a cross-reference to section 28 (national security and defence: modifications to Articles 9 and 32 of the applied GDPR).

759 Paragraph 47 modifies Article 58 of the GDPR (powers) for the applied GDPR to omits the reference to the controller or processor's representative and replace references to "Union or Member State procedural law" and "the Member State government" with references to "domestic law" and "the Secretary of State" respectively. It also omits paragraphs 3(c) (power in relation to Article 36(5)) (see paragraph 28 of this Schedule), 4 (requirement on Member States to provide appropriate safeguards), 5 (requirement on Member States to provide for judicial remedies) and 6 (ability of Member States to provide the supervisory authority with

additional powers).

760 Paragraph 48 modifies Article 59 of the GDPR (activity reports) to replace the reference to "the Government and other authorities as designated by Member State law" with a reference to the Secretary of State; and to omit references to the European Commission and European Data Protection Board.

761 Paragraph 49 replaces Articles 60 to 76 of the GDPR (co-operation and consistency) with a much shorter replacement Article (new Article 61) in the applied GDPR. This Article explains how the Commissioner can cooperate with other supervisory authorities, including by conducting joint operations, and how the Commissioner should have regard to the activities of the European Data Protection Board under Article 68 of the GDPR, and any implementing acts adopted by the European Commission under Article 67 of the GDPR (exchange of information).

762 Paragraph 50 modifies Article 77 of the GDPR (right to lodge a complaint with a supervisory authority) for the applied GDPR to remove references to cross-border application.

763 Paragraph 51 modifies Article 78 of the GDPR (right to an effective judicial remedy against a supervisory authority) for the applied GDPR to remove provision relating to cross-border application and to omit paragraph 4 (requirement to forward opinions and decisions of the European Data Protection Board).

764 Paragraph 52 modifies Article 79 of the GDPR (right to an effective judicial remedy against a controller or processor) for the applied GDPR to remove the reference to cross-border application.

765 Paragraph 53 modifies Article 80 of the GDPR (representation of data subjects) for the applied GDPR to omit the reference to "where provided for by Member State law" from paragraph 1 and to replace the reference to "Member States" in paragraph 2 (ability of Member States to make additional provision) with a reference to the Secretary of State. Paragraph 53(c) clarifies that the Secretary of State may only exercise that power by making regulations under section 190 of the Act (see above).

766 Paragraph 54 omits Article 81 of the GDPR (suspension of proceedings) from the applied GDPR.

767 Paragraph 55 modifies Article 82 of the GDPR (right to compensation and liability) for the applied GDPR to replace the reference to "the courts competent under the law of the Member State" with reference to "a court".

768 Paragraph 56 modifies Article 83 of the GDPR (general conditions for imposing administrative fines) for the applied GDPR to replace references to "Member States" and "Member State law" with references to this Act, "the Secretary of State" or "the United Kingdom" as appropriate. It also replaces paragraph 8 (requirement on Member States to provide appropriate procedural safeguards) with a cross reference to relevant provision of this Act, and omits paragraph 9 (provision in respect of Member States whose legal systems do not provide for administrative fines).

769 Paragraph 57 modifies Article 84 (penalties) for the applied GDPR to replace paragraph 1 (requirement on Member States to lay down rules on other others) with a reference to the Act. It also omits paragraph 2 (requirement to notify to the European Commission).

770 Paragraph 58 modifies Article 85 of the GDPR (processing and freedom of expression and information) for the applied GDPR to omit paragraphs 1 (requirement on Member States to reconcile the right to the protection of personal data with the right to freedom of expression

and information) and 3 (requirement to notify to the European Commission), replace references to "Member States shall" with references to "the Secretary of State may", and add a cross reference to relevant provisions in this Act.

771 Paragraph 59 modifies Article 86 of the GDPR (processing and public access to official documents) for the applied GDPR to replace the reference to "Union or Member State law to which the public authority or body is subject" with reference to "domestic law".

772 Paragraph 60 omits Article 87 (processing of national identification number) from the applied GDPR.

773 Paragraph 61 omits Article 88 of the GDPR (processing in the context of employment) from the applied GDPR.

774 Paragraph 62 modifies Article 89 of the GDPR (safeguards and derogations relating processing for archiving purposes etc) for the applied GDPR to replace references to "Union or Member State law" with references to "the Secretary of State", and to replace the reference to "relevant provisions" with references to this Act.

775 Paragraph 63 omits Article 90 of the GDPR (obligations of secrecy) from the applied GDPR.

776 Paragraph 64 omits Article 91 of the GDPR (existing data protection rules of churches and religious associations) from the applied GDPR.

777 Paragraph 65 omits Article 92 (exercise of the delegation) from the applied GDPR.

778 Paragraph 66 omits Article 93 (committee procedure) from the applied GDPR.

779 Paragraph 67 omits Article 94 (repeal of Directive 95/46/EC) from the applied GDPR.

780 Paragraph 68 omits Article 95 (relationship with Directive 2002/58/EC) from the applied GDPR.

781 Paragraph 69 modifies Article 96 of the GDPR (relationship with previously concluded Agreements) for the applied GDPR to replace references to "Member States" with references to "the United Kingdom or the Commissioner".

782 Paragraph 70 omits Article 97 (Commission reports) from the applied GDPR.

783 Paragraph 71 omits Article 98 (Commission reviews) from the applied GDPR.

784 Paragraph 72 omits Article 99 (entry into force and application) from the applied GDPR.

785 In Part 2, paragraph 73 introduces paragraphs 74 and 75 (modifications to Chapter 2 of Part 2).

786 Paragraph 74 provides that the applied Chapter 2 should be interpreted identically to the regular Chapter 2, except that references to Chapter 2 are to be read as references to the applied Chapter 2; references to the GDPR are to be read as references to the applied GDPR; and references to data which is in-scope of Chapter 2 of Part 2 are to be read as references to data which is in-scope of Chapter 3 of Part 2. One exception is provided: the reference in section 18 to Article 45(3) of the GDPR should continue to be interpreted as a reference to the GDPR and not the applied GDPR.

787 Paragraph 75 establishes one further difference between Chapter 2 and the applied Chapter 2. It provides that, in the applied Chapter 2, the reference in section 16 to "Member State law" should be replaced with a reference to "the Secretary of State".

Schedule 7: Competent authorities

788 This Schedule sets out a list of competent authorities for the purposes of Part 3 of the Act; this

is to be read in conjunction with section 30. An office holder or body listed as a competent authority are only a competent authority in relation to the processing of personal data carried out for a law enforcement purpose.

Schedule 8: Conditions for sensitive processing under Part 3

789 This Schedule sets out the conditions for sensitive processing under Part 3 of the Act. These include judicial and statutory purposes, protecting individuals' vital interests, safeguarding of children and of individuals at risk, personal data in the public domain, legal claims and judicial acts, prevention of fraud and archiving.

Schedule 9: Conditions for processing under Part 4

790 This Schedule sets out the relevant conditions for the lawful processing of sensitive personal data under Part 4.

Schedule 10: Conditions for sensitive processing under Part 4

791 This Schedule sets out the relevant conditions for lawful and fair sensitive processing under Part 4.

Schedule 11: Other exemptions under Part 4

792 This Schedule provides for exemptions under Part 4 to:

- the data protection principles set out in Part 4 of the Act, except where they require compliance with condition that the processing is lawful, as set out in section 86(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.

793 Paragraph 2 provides an exemption in relation to the prevention of crime.

794 Paragraph 3 provides exemptions in relation to disclosures required by law or in connection with legal proceedings or obtaining legal advice.

795 Paragraph 4 provides an exemption in relation to Parliamentary privilege.

796 Paragraph 5 provides an exemption in relation to judicial proceedings.

797 Paragraph 6 provides exemptions in relation to Crown honours and dignities.

798 Paragraph 7 provides exemptions in relation to the any prejudice to the combat effectiveness of the armed forces.

799 Paragraph 8 provides exemptions in relation to circumstances likely to prejudice of the economic wellbeing of the United Kingdom.

800 Paragraph 9 provides exemptions in relation to legal professional privilege.

801 Paragraph 10 provides exemptions in relation to negotiations.

802 Paragraph 11 provides exemptions in relation to confidential references given by the

controller.

803 Paragraph 12 provides exemptions in relation to exam scripts and marks.

804 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.

805 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

806 This Schedule makes provision about the Commissioner. It substantively replicates Schedule 5 to the 1998 Act.

807 Paragraph 1 provides that the Commissioner will continue to be a corporation sole.

808 Paragraph 2 makes provision about the process for appointing the Commissioner and about the maximum length of an appointment. The Commissioner must be appointed on the basis of merit following an open and fair competition.

809 Paragraph 3 makes provision about how the Commissioner may resign or be removed from office.

810 Paragraph 4 makes provision about the Commissioner's pay and pension.

811 Paragraph 5 requires the Commissioner to appoint one or more deputy commissioners and empowers her to appoint other staff, having regard to the principles of open and fair competition.

812 Paragraph 6 makes provision for the carrying out of the Commissioner's functions by officers and staff.

813 Paragraph 7 makes provision about the authentication of the Commissioner's seal.

814 Paragraph 8 makes provision for the presumption of authenticity of documents issued by the Commissioner.

815 Paragraph 9 is self-explanatory.

816 Paragraph 10 requires fees, charges and penalties received by the Commissioner in the course of carrying out the Commissioner's functions to be paid to the Secretary of State, unless the Secretary of State, with the consent of the Treasury, directs otherwise. The Secretary of State must pay any sums received under this paragraph to the Consolidated Fund.

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

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

Schedule 13: Other general functions of the Commissioner

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

- monitor and enforce Parts 3 and 4 of the Act. 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 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 Act;
- monitor developments that impact on the protection of personal data; and
- contribute to the activities of the European Data Protection Board.

820 This Schedule also provides the Commissioner 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: Co-operation and mutual assistance

821 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 LED and compliance with Convention 108.

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

823 A "foreign designated authority" is an authority, in a state other than the UK and which is bound by Convention 108, responsible for Convention 108.

824 Part 1 of the Schedule sets out the functions of the Commissioner with respect to Article 50 of the LED 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.

825 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.

826 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.

827 Paragraph 2 sets out how the Commissioner should respond to a request from an LED supervisory authority for information or assistance.

828 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. Section 134 (fees) sets out the power for the Commissioner to charge a fee for other services.

829 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.

830 Part 2 of the Schedule sets out the functions of the Commissioner with respect to Article 13 of Convention 108 and cooperating with foreign designated authorities. This replaces the provision of the Data Protection (Functions of Designated Authority) Order 2000 (S.I. 2000/186).

831 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.

832 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 Convention 108.

833 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

834 This Schedule makes provision in respect of the Commissioner's powers of entry and inspection. It substantively replicates Schedule 9 to the 1998 Act.

835 Paragraph 1 sets out the circumstances in which a circuit judge, a District Judge (Magistrates' Court) or a judge of the High Court may grant a warrant to the Commissioner other than in connection with assessment notices.

836 Paragraph 2 gives the court the power to issue warrants in connection with assessment notices.

837 Paragraph 3 prevents a judge from issuing a warrant if the processing is required for special purposes (i.e. for the purposes of journalism or academic, artistic or literary purposes) unless a determination under section 174 with respect to the data or the processing has taken effect.

838 Paragraph 4 provides restrictions and conditions which a Judge must consider and be satisfied have been met before issuing a warrant. A Judge may only issue a warrant if satisfied that one or more of the requirements within paragraph 4(1) is met. In order for the requirement under paragraph 4(1)(a) to be satisfied, the three conditions within paragraph 4, sub-paragraphs (2) to (4) must be met. Alternatively, the judge must be satisfied that the Information Commissioner requires urgent access to the premises and/or compliance with the conditions in question would defeat the object of entry into the premises in question.

839 Paragraph 5 makes provision as to the content of warrants. A warrant must, among other matters, authorise the Commissioner to enter and search premises and inspect and seize documents.

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

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

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

843 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.

844 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.

845 Paragraphs 11 and 12 exempts from seizure certain privileged communications.

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

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

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

849 Paragraph 16 sets out the circumstances 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.

850 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.

851 Paragraph 18 makes provision relating to the application of this Schedule to Scotland. Paragraph 19 does the same for Northern Ireland.

Schedule 16: Penalties

852 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.

853 Paragraph 1 defines the meaning of a "penalty".

854 Paragraph 2 explains that the Commissioner must give a "notice of intent" to the person to whom they intend to issue a penalty notice. The Commissioner cannot issue a penalty notice after six months has passed from the date they issued the written notice, unless the Commissioner and the person receiving the notice of intent have agreed an extension.

855 Paragraph 3 explains what the Commissioner must include in the notice of intent. This includes an indication of the amount of the penalty, the nature of the offence, the period in which the person can make written representations about the Commissioner's intention to issue a penalty notice, and whether a controller or processor can make oral representations.

856 Paragraph 4 states that the Commissioner must first consider any oral or written representations by the person, 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 person has passed before issuing a penalty notice.

857 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.

858 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.

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

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

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

Schedule 17: Review of processing of personal data for the purposes of journalism

862 This Schedule provides the Information Commissioner with additional powers during any review period when conducting a review as required under section 178.

863 Paragraph 2 provides the Commissioner with the ability to apply a modified form of the urgent procedure to information notices that she gives for the purpose of the review. The effect of this is that the minimum time period that the Commissioner must give is reduced to 24 hours (but see paragraph 4). Nothing in paragraph 2 affects the application of section 143 (information notices: restrictions).

864 Section 147(5) prevents the Commissioner from giving an assessment notice with respect to the processing of personal data for the special purposes. Paragraph 3 of this Schedule disapplies section 147(5), providing the Commissioner with the ability to give assessment notices for the purpose of the review, but only where a determination under section 174 has taken effect. This requirement is comparable to the restriction on the giving of information notices set out in section 143(1).

865 Paragraph 4 makes clear that section 164 (applications in respect of urgent notices) applies in respect of information and assessment notices given under paragraphs 2 and 3.

Schedule 18: Relevant records

866 This Schedule explains the meaning of "relevant records" for the purposes of the offence in section 184 (prohibition of requirement to produce relevant records).

867 Paragraph 1 states that "relevant records" includes health records, records relevant to a conviction or a caution and records relating to statutory functions.

868 Relevant health records are defined in paragraph 2. Records relating to convictions and cautions are defined in paragraph 3. Records relating to statutory functions are defined in paragraph 4.

869 Paragraph 5 sets out the meaning of "data subject access rights" for the purposes of this Schedule and the offence in section 184.

870 Paragraph 6 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.

871 Paragraph 7 provides the Secretary of State with a power to amend this Schedule via the affirmative resolution procedure.

Schedule 19: Minor and consequential amendments

872 This Schedule repeals the 1998 Act, and makes amendments to other legislation which are

necessary to reflect both the repeal of the 1998 Act and the requirements of the GDPR. The explanatory notes will provide an overview of these amendments, but will not explain every amendment in detail.

873 Often pieces of legislation refer to other legislation. One of the purposes this Schedule has is to make sure such references continue to work despite the other changes made by this Act. The Schedule also updates certain definitions to refer to definitions in this Act, for example where reference was made to the definition of "personal data" as defined in section 1 of the 1998 Act, this will now refer to the definition in section 3 of this Act.

874 This Schedule makes a number of very similar amendments. For example there are a number of provisions in other legislation which require disclosure of information, but which state that such a duty does not apply where it would contravene the requirements of the 1998 Act. Schedule 19 amends these references to make it clear that the requirement to disclose information does not apply if doing so would breach any requirements or restrictions under the data protection legislation as defined in this Act. Such amendments are made in paragraphs 96, 159, 208 and 220 (among others).

875 A number of the amendments listed in this Schedule relate to provisions in other legislation which require other bodies to provide personal data to the Information Commissioner which is required for her to fulfil her enforcement duties under this Act. See paragraphs 3, 4, 87, 168 and 204 for example.

876 There were also a number of references in other legislation to the "non-disclosure" provisions as set out in section 27(3) of the 1998 Act. The "non-disclosure" provisions referred to exemptions under the 1998 Act which permitted disclosure of personal data where this would otherwise be prohibited. The references in other legislation most often referred to the exemption under section 35 of the 1998 Act (exemption for cases where disclosure is required by law).

877 Although the "non-disclosure" provisions have not been replicated in the same way in the Act, in order to ensure the references in other legislation continue to function appropriately, the references have been updated to refer to either the provisions which can be exempt as listed in paragraph 1 of Schedule 2 to the Act, or to paragraph 5(3) of Schedule 2 which replaces the exemption in section 35 of the 1998 Act. Examples of such amendments can be found in paragraphs 19 to 30and 35 of this Schedule.

878 Paragraphs 55 to 64 amend the 2000 Act to reflect the provisions of the GDPR.

879 In particular, paragraph 58 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 (Article 5) 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.

880 Paragraph 59 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 section 140 of this Act which introduces a general requirement for the Information Commissioner to publish annual reports on his/her functions.

881 Paragraph 60 mirrors the provisions on contempt of court in section 202 of this Act to ensure they apply to FOI proceedings.

882 Paragraph 63 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 section 173 of this Act.

883 Paragraphs 88 to 90 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.

884 Paragraph 150 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 sections 170 and 196 of this Act.

885 Paragraph 224 omits sections 108 to 110 of the Digital Economy Act 2017 which is concerned with charges payable to the Information Commissioner. These provisions have been superseded by section 137 of this Act. Paragraph 26 of Schedule 20 makes transitional provision.

886 Paragraphs 305 to 309 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. Similar amendments are made to other subordinate legislation by paragraphs 310 to 312.

887 Paragraph 380 omits Part 4 of the Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014 (S.I. 2014/3141), which sets rules for data processing by competent authorities based on the requirements of the 1998 Act. This Part is now redundant.

888 Paragraph 434 provides that provisions added to secondary legislation by this Schedule can be amended by powers under the legislation they amended.

Schedule 20: Transitional provision etc

889 This Schedule makes provision in relation to matters such as the rights of access to personal data under the 1998 Act following the repeal of that Act.

890 Part 1 makes provision defining terms used in this Schedule.

891 Part 2 of this Schedule is about the rights of data subjects.

892 Paragraph 2 makes provision for sections 7 to 9A of the 1998 Act to be preserved in relation to requests made under section 7 before its repeal. It makes similar provision in relation to sections 7 and 8 of the 1998 Act as modified by the Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014 (S.I. 2014/3141) so that requests made under section 7 are unaffected notwithstanding the revocation of those regulations.

893 Paragraph 3 makes provision preserving section 10 of the 1998 Act in relation to the exercise of the right to prevent processing likely to cause damage or distress under that section before its repeal.

894 Paragraph 4 makes provision preserving section 11 of the 1998 Act in relation to the exercise of the right to prevent processing for the purposes of direct marketing under that section before its repeal.

895 Paragraph 5 makes provision preserving section 12 of the 1998 Act in relation to the exercise of rights in respect of a decision taken before the repeal of that section.

896 Paragraph 6 makes provision for section 13 of the 1998 Act to be preserved in relation to a

claim for damage or distress caused by an act or omission occurring before the repeal of that section. Similar provision is made preserving regulation 45 of the Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014 (S.I. 2014/3141) in relation to a claim for compensation connected to an act or omission occurring before the revocation of that regulation.

897 Paragraph 7 provides for section 14 of the 1998 Act to be preserved in relation to an application for the rectification, blocking, erasure or destruction of inaccurate personal data made before the repeal of that section.

898 Paragraph 8 makes provision which preserves section 15 of the 1998 Act as it applies in connection with sections 7 to 14 as preserved by this Schedule.

899 Paragraph 9 preserves Part 4 of the 1998 Act so that it continues to apply in connection with a provision of Part 2 of that Act as preserved by paragraphs 2 to 7 of this Schedule. It also preserves secondary legislation made under Part 4 of the 1998 Act as that legislation applies in connection with a preserved provision of Part 2 of that Act.

900 Paragraph 10 clarifies for transitional purposes provision relating to the avoidance under this Act of certain contractual terms relating to health records.

901 Part 3 of this Schedule makes transitional provision relating to the interaction between the GDPR and Part 2 of this Act, namely exemptions from the GDPR in the form of restrictions of rules in Articles 13 to 15 of that Regulation and manual unstructured data held by FOI public authorities.

902 Part 4 of this Schedule makes transitional provision in relation to law enforcement and intelligence services processing, namely logging, regulation 50 of the Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014 (S.I. 2014/3141) and the maximum fee for data subject access requests to intelligence services. In particular, paragraph 19 delays the requirement to comply the logging provisions set out under section 62 until 6 May 2023 for any automated processing system which was in place prior to 6 May 2016 where to comply would involve a disproportionate effort.

903 Part 5 of this Schedule makes transitional provision in relation to national security certificates.

904 Part 6 of this Schedule provides for a number of matters relating to the Commissioner including the continuation of the appointment of the existing Commissioner.

905 Part 7 of this Schedule is about enforcement under the 1998 Act. This Part provides for those sections of the 1998 Act which are concerned with information notices, special information notices, assessment notices, enforcement notices and penalty notices to continue to have effect for transitional purposes after their repeal. Transitional provision is also made in relation to matters such as offences, powers of entry and appeals under the 1998 Act. Modifications to the provisions concerned made by the Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014 (S.I. 2014/3141) continue to have effect by virtue of the preservation of regulation 51 by this Part for these purposes.

906 Part 8 of this Schedule is about enforcement under this Act and makes provision clarifying the reference to offences in this Act and the position in relation to the Tribunal Procedure Rules made under the 1998 Act.

907 Part 9 makes transitional provision in relation to other enactments such as various powers to disclose information to the Commissioner.

Commencement

908 The following provisions of the Act will come into force on Royal Assent: sections 1 (overview) and 3 (terms relating to the processing of personal data); 182 (regulations and consultation), 204 to 206 (definitions); 209 and 210 (application to the Crown and Parliament); 212, 213(2), 214 and 215 (final provisions); and all powers to make secondary legislation.

909 The following provisions of the Act will come into force at the end of the period of 2 months from the date of Royal Assent: sections 124, and 125, 126 and 127, so far as they relate to a code prepared under section 124 (data protection and journalism code); section 177 (guidance about how to seek redress against media organisations); section 178 and Schedule 17 (review of processing of personal data for the purposes of journalism); and section 179 (effectiveness of the media's dispute resolution procedures).

910 The other provisions of the Act will be brought into force by regulations made by the Secretary of State.

Financial implications of the Act

911 The financial costs and benefits of the Act have been set out in accompanying impact assessments. The following assessments have been made:

- Data Protection Bill: summary assessment;
- Data Protection Bill (general processing);
- Data Protection Bill: implementing the European Union Law Enforcement Directive.

Related documents

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

http://www.gov.uk/Government/collections/data-protection-act-2018

913 The following documents are relevant to the Act,

- The GDPR;
- The LED;
- The 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;
- General processing Impact Assessment;

- Law Enforcement Directive Impact Assessment;
- Equality Impact Assessment; and
- 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.
Modernised Convention 108	The modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, as adopted by the Committee of Ministers of the Council of Europe on 18 May 2018.
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 ((EU) 2016/679)
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.
PECR	Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426)
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 1995 Directive	European Data Protection Directive (Directive 95/46/EC)
The 1998 Act	Data Protection Act 1998
The 2000 Act	Freedom of Information Act 2000
The 2016 Act	Investigatory Powers Act 2016
The Commissioner	The Information Commissioner

Annex B – Territorial extent and application in the United Kingdom

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?
Sections 1 to 187	Yes	Yes	Yes	Yes
Sections 188 to 190	Yes	Yes	No	Yes
Sections 191 to 198	Yes	Yes	Yes	Yes
Sections 199 and 200	Yes	Yes	No	No
Sections 201 to 207	Yes	Yes	Yes	Yes
Section 208	No	No	Yes	No
Section 209 to 215	Yes	Yes	Yes	Yes
Schedules 1 to 11	Yes	Yes	Yes	Yes
Schedule 12	Yes	Yes	Yes (subject to paragraph 12 of Schedule 12)	Yes
Schedules 13 to 17	Yes	Yes	Yes	Yes
Schedules 19 and 20	In part	In part	In part	In part

Annex C – Hansard References

914 The following table sets out the dates and Hansard references for each stage of the Act's passage through Parliament.

Stage	Date	Hansard Reference
House of Lords		
Introduction	13 September 2017	Vol. 783 Col. 2457
Second Reading	10 October 2017	Vol. 785 Col. 124
Committee	30 October 2017 6 November 2017 13 November 2017 15 November 2017 20 November 2017 22 November 2017	Vol. 785 Col. 1161 Vol. 785 Col. 1578 Vol. 785 Col. 1804 Vol. 785 Col. 2031 Vol. 787 Col. 13 Vol. 787 Col. 177
Report	11 December 2017 13 December 2017 10 January 2018	Vol. 787 Col. 1378 Vol. 787 Col. 1556 Vol. 788 Col. 192
Third Reading	17 January 2018	Vol. 788 Col. 648
House of Commons		
Introduction	18 January 2018	Votes and Proceedings No.81 of 2017-19
Second Reading	5 March 2018	Vol. 637 Col. 75
Public Bill Committee	13 March 2018 15 March 2018 20 March 2018 22 March 2018	PBC (Bill 153) 2017 - 2019
Report and Third Reading	9 May 2018	Vol. 640 Col. 700
Lords Consideration of Commons Amendments	14 May 2018	Vol. 791 Col. 415
Commons Consideration of Lords Messages	15 May 2018	Vol. 641 Col. 168
Lords Consideration of Commons Disagreement	21 May 2018	Vol. 791 Col. 878
Royal Assent	23 May 2018	House of Lords – Vol. 791 Col. 1023 House of Commons – Vol 641 Col. 903

Annex D – Progress of Bill Table

This Annex shows how each section and Schedule of the Act was numbered during the passage of the Bill through Parliament.

Section of the Act	Bill as introduced in the Lords	Bill as amended in Committee in the Lords	Bill as amended on Report in the Lords	Bill as brought from the Lords	Bill as amended in Public Bill Committee in the Commons
Section 1	Clause 1	Clause 1	Clause 1	Clause 1	Clause 1
Section 2			Clause 2	Clause 2	Clause 2
Section 3	Clause 2	Clause 2	Clause 3	Clause 3	Clause 3
Section 4	Clause 3	Clause 3	Clause 4	Clause 4	Clause 4
Section 5	Clause 4	Clause 4	Clause 5	Clause 5	Clause 5
Section 6	Clause 5	Clause 5	Clause 6	Clause 6	Clause 6
Section 7	Clause 6	Clause 6	Clause 7	Clause 7	Clause 7
Section 8	Clause 7	Clause 7	Clause 8	Clause 8	Clause 8
Section 9	Clause 8	Clause 8	Clause 9	Clause 9	Clause 9
Section 10	Clause 9	Clause 9	Clause 10	Clause 10	Clause 10
Section 11	Clause 10	Clause 10	Clause 11	Clause 11	Clause 11
Section 12	Clause 11	Clause 11	Clause 12	Clause 12	Clause 12
Section 13	Clause 12	Clause 12	Clause 13	Clause 13	Clause 13
Section 14	Clause 13	Clause 13	Clause 14	Clause 14	Clause 14
Section 15	Clause 14	Clause 14	Clause 15	Clause 15	Clause 15
Section 16	Clause 15	Clause 15	Clause 16	Clause 16	Clause 16
Section 17	Clause 16	Clause 16	Clause 17	Clause 17	Clause 17
Section 18	Clause 17	Clause 17	Clause 18	Clause 18	Clause 18
Section 19	Clause 18	Clause 18	Clause 19	Clause 19	Clause 19
Section 20			Clause 20	Clause 20	Clause 20
Section 21	Clause 19	Clause 19	Clause 21	Clause 21	Clause 21
Section 22	Clause 20	Clause 20	Clause 22	Clause 22	Clause 22
Section 23	Clause 21	Clause 21	Clause 23	Clause 23	Clause 23
Section 24	Clause 22	Clause 22	Clause 24	Clause 24	Clause 24
Section 25	Clause 23	Clause 23	Clause 25	Clause 25	Clause 25
Section 26	Clause 24	Clause 24	Clause 26	Clause 26	Clause 26
Section 27	Clause 25	Clause 25	Clause 27	Clause 27	Clause 27
Section 28	Clause 26	Clause 26	Clause 28	Clause 28	Clause 28
Section 29	Clause 27	Clause 27	Clause 29	Clause 29	Clause 29
Section 30	Clause 28	Clause 28	Clause 30	Clause 30	Clause 30

Section of the Act	Bill as introduced in the Lords	Bill as amended in Committee in the Lords	Bill as amended on Report in the Lords	Bill as brought from the Lords	Bill as amended in Public Bill Committee in the Commons
Section 31	Clause 29	Clause 29	Clause 31	Clause 31	Clause 31
Section 32	Clause 30	Clause 30	Clause 32	Clause 32	Clause 32
Section 33	Clause 31	Clause 31	Clause 33	Clause 33	Clause 33
Section 34	Clause 32	Clause 32	Clause 34	Clause 34	Clause 34
Section 35	Clause 33	Clause 33	Clause 35	Clause 35	Clause 35
Section 36	Clause 34	Clause 34	Clause 36	Clause 36	Clause 36
Section 37	Clause 35	Clause 35	Clause 37	Clause 37	Clause 37
Section 38	Clause 36	Clause 36	Clause 38	Clause 38	Clause 38
Section 39	Clause 37	Clause 37	Clause 39	Clause 39	Clause 39
Section 40	Clause 38	Clause 38	Clause 40	Clause 40	Clause 40
Section 41	Clause 39	Clause 39	Clause 41	Clause 41	Clause 41
Section 42	Clause 40	Clause 40	Clause 42	Clause 42	Clause 42
Section 43	Clause 41	Clause 41	Clause 43	Clause 43	Clause 43
Section 44	Clause 42	Clause 42	Clause 44	Clause 44	Clause 44
Section 45	Clause 43	Clause 43	Clause 45	Clause 45	Clause 45
Section 46	Clause 44	Clause 44	Clause 46	Clause 46	Clause 46
Section 47	Clause 45	Clause 45	Clause 47	Clause 47	Clause 47
Section 48	Clause 46	Clause 46	Clause 48	Clause 48	Clause 48
Section 49	Clause 47	Clause 47	Clause 49	Clause 49	Clause 49
Section 50	Clause 48	Clause 48	Clause 50	Clause 50	Clause 50
Section 51	Clause 49	Clause 49	Clause 51	Clause 51	Clause 51
Section 52	Clause 50	Clause 50	Clause 52	Clause 52	Clause 52
Section 53	Clause 51	Clause 51	Clause 53	Clause 53	Clause 53
Section 54	Clause 52	Clause 52	Clause 54	Clause 54	Clause 54
Section 55	Clause 53	Clause 53	Clause 55	Clause 55	Clause 55
Section 56	Clause 54	Clause 54	Clause 56	Clause 56	Clause 56
Section 57	Clause 55	Clause 55	Clause 57	Clause 57	Clause 57
Section 58	Clause 56	Clause 56	Clause 58	Clause 58	Clause 58
Section 59	Clause 57	Clause 57	Clause 59	Clause 59	Clause 59
Section 60	Clause 58	Clause 58	Clause 60	Clause 60	Clause 60
Section 61	Clause 59	Clause 59	Clause 61	Clause 61	Clause 61
Section 62	Clause 60	Clause 60	Clause 62	Clause 62	Clause 62
Section 63	Clause 61	Clause 61	Clause 63	Clause 63	Clause 63
Section 64	Clause 62	Clause 62	Clause 64	Clause 64	Clause 64

Section of the Act	Bill as introduced in the Lords	Bill as amended in Committee in the Lords	Bill as amended on Report in the Lords	Bill as brought from the Lords	Bill as amended in Public Bill Committee in the Commons
Section 65	Clause 63	Clause 63	Clause 65	Clause 65	Clause 65
Section 66	Clause 64	Clause 64	Clause 66	Clause 66	Clause 66
Section 67	Clause 65	Clause 65	Clause 67	Clause 67	Clause 67
Section 68	Clause 66	Clause 66	Clause 68	Clause 68	Clause 68
Section 69	Clause 67	Clause 67	Clause 69	Clause 69	Clause 69
Section 70	Clause 68	Clause 68	Clause 70	Clause 70	Clause 70
Section 71	Clause 69	Clause 69	Clause 71	Clause 71	Clause 71
Section 72	Clause 70	Clause 70	Clause 72	Clause 72	Clause 72
Section 73	Clause 71	Clause 71	Clause 73	Clause 73	Clause 73
Section 74	Clause 72	Clause 72	Clause 74	Clause 74	Clause 74
Section 75	Clause 73	Clause 73	Clause 75	Clause 75	Clause 75
Section 76	Clause 74	Clause 74	Clause 76	Clause 76	Clause 76
Section 77	Clause 75	Clause 75	Clause 77	Clause 77	Clause 77
Section 78	Clause 76	Clause 76	Clause 78	Clause 78	Clause 78
Section 79	Clause 77	Clause 77	Clause 79	Clause 79	Clause 79
Section 80	Clause 78	Clause 78	Clause 80	Clause 80	Clause 80
Section 81	Clause 79	Clause 79	Clause 81	Clause 81	Clause 81
Section 82	Clause 80	Clause 80	Clause 82	Clause 82	Clause 82
Section 83	Clause 81	Clause 81	Clause 83	Clause 83	Clause 83
Section 84	Clause 82	Clause 82	Clause 84	Clause 84	Clause 84
Section 85	Clause 83	Clause 83	Clause 85	Clause 85	Clause 85
Section 86	Clause 84	Clause 84	Clause 86	Clause 86	Clause 86
Section 87	Clause 85	Clause 85	Clause 87	Clause 87	Clause 87
Section 88	Clause 86	Clause 86	Clause 88	Clause 88	Clause 88
Section 89	Clause 87	Clause 87	Clause 89	Clause 89	Clause 89
Section 90	Clause 88	Clause 88	Clause 90	Clause 90	Clause 90
Section 91	Clause 89	Clause 89	Clause 91	Clause 91	Clause 91
Section 92	Clause 90	Clause 90	Clause 92	Clause 92	Clause 92
Section 93	Clause 91	Clause 91	Clause 93	Clause 93	Clause 93
Section 94	Clause 92	Clause 92	Clause 94	Clause 94	Clause 94
Section 95	Clause 93	Clause 93	Clause 95	Clause 95	Clause 95
Section 96	Clause 94	Clause 94	Clause 96	Clause 96	Clause 96
Section 97	Clause 95	Clause 95	Clause 97	Clause 97	Clause 97
Section 98	Clause 96	Clause 96	Clause 98	Clause 98	Clause 98

Section of the Act	Bill as introduced in the Lords	Bill as amended in Committee in the Lords	Bill as amended on Report in the Lords	Bill as brought from the Lords	Bill as amended in Public Bill Committee in the Commons
Section 99	Clause 97	Clause 97	Clause 99	Clause 99	Clause 99
Section 100	Clause 98	Clause 98	Clause 100	Clause 100	Clause 100
Section 101	Clause 99	Clause 99	Clause 101	Clause 101	Clause 101
Section 102	Clause 100	Clause 100	Clause 102	Clause 102	Clause 102
Section 103	Clause 101	Clause 101	Clause 103	Clause 103	Clause 103
Section 104	Clause 102	Clause 102	Clause 104	Clause 104	Clause 104
Section 105	Clause 103	Clause 103	Clause 105	Clause 105	Clause 105
Section 106	Clause 104	Clause 104	Clause 106	Clause 106	Clause 106
Section 107	Clause 105	Clause 105	Clause 107	Clause 107	Clause 107
Section 108	Clause 106	Clause 106	Clause 108	Clause 108	Clause 108
Section 109	Clause 107	Clause 107	Clause 109	Clause 109	Clause 109
Section 110	Clause 108	Clause 108	Clause 110	Clause 110	Clause 110
Section 111	Clause 109	Clause 109	Clause 111	Clause 111	Clause 111
Section 112	Clause 110	Clause 110	Clause 112	Clause 112	Clause 112
Section 113	Clause 111	Clause 111	Clause 113	Clause 113	Clause 113
Section 114	Clause 112	Clause 112	Clause 114	Clause 114	Clause 114
Section 115	Clause 113	Clause 113	Clause 115	Clause 115	Clause 115
Section 116	Clause 114	Clause 114	Clause 116	Clause 116	Clause 116
Section 117	Clause 115	Clause 115	Clause 117	Clause 117	Clause 117
Section 118	Clause 116	Clause 116	Clause 118	Clause 118	Clause 118
Section 119	Clause 117	Clause 117	Clause 119	Clause 119	Clause 119
Section 120	Clause 118	Clause 118	Clause 120	Clause 120	Clause 120
Section 121	Clause 119	Clause 119	Clause 122	Clause 122	Clause 121
Section 122	Clause 120	Clause 120	Clause 123	Clause 123	Clause 122
Section 123			Clause 124	Clause 124	Clause 123
Section 124					
Section 125	Clause 121	Clause 121	Clause 125	Clause 125	Clause 124
Section 126	Clause 122	Clause 122	Clause 126	Clause 126	Clause 125
Section 127	Clause 123	Clause 123	Clause 127	Clause 127	Clause 126
Section 128	Clause 124	Clause 124	Clause 128	Clause 128	Clause 127
Section 129	Clause 125	Clause 125	Clause 129	Clause 129	Clause 128
Section 130			Clause 130	Clause 130	Clause 129
Section 131	Clause 126	Clause 126	Clause 131	Clause 131	Clause 130
Section 132	Clause 127	Clause 127	Clause 132	Clause 132	Clause 131

Section of the Act	Bill as introduced in the Lords	Bill as amended in Committee in the Lords	Bill as amended on Report in the Lords	Bill as brought from the Lords	Bill as amended in Public Bill Committee in the Commons
Section 133	Clause 128	Clause 128	Clause 133	Clause 133	Clause 132
Section 134	Clause 129	Clause 129	Clause 134	Clause 134	Clause 133
Section 135	Clause 130	Clause 130	Clause 135	Clause 135	Clause 134
Section 136	Clause 131	Clause 131	Clause 136	Clause 136	Clause 135
Section 137	Clause 132	Clause 132	Clause 137	Clause 137	Clause 136
Section 138	Clause 133	Clause 133	Clause 138	Clause 138	Clause 137
Section 139	Clause 134	Clause 134	Clause 139	Clause 139	Clause 138
Section 140	Clause 135	Clause 135	Clause 140	Clause 140	Clause 139
Section 141	Clause 136	Clause 136	Clause 141	Clause 141	Clause 140
Section 142	Clause 137	Clause 137	Clause 143	Clause 143	Clause 141
Section 143	Clause 138	Clause 138	Clause 144	Clause 144	Clause 142
Section 144	Clause 139	Clause 139	Clause 145	Clause 145	Clause 143
Section 145					
Section 146	Clause 140	Clause 140	Clause 146	Clause 146	Clause 144
Section 147	Clause 141	Clause 141	Clause 147	Clause 147	Clause 145
Section 148					
Section 149	Clause 142	Clause 142	Clause 148	Clause 148	Clause 146
Section 150	Clause 143	Clause 143	Clause 149	Clause 149	Clause 147
Section 151	Clause 144	Clause 144	Clause 150	Clause 150	Clause 148
Section 152	Clause 145	Clause 145	Clause 151	Clause 151	Clause 149
Section 153	Clause 146	Clause 146	Clause 152	Clause 152	Clause 150
Section 154	Clause 147	Clause 147	Clause 153	Clause 153	Clause 151
Section 155	Clause 148	Clause 148	Clause 154	Clause 154	Clause 152
Section 156	Clause 149	Clause 149	Clause 155	Clause 155	Clause 153
Section 157	Clause 150	Clause 150	Clause 156	Clause 156	Clause 154
Section 158	Clause 151	Clause 151	Clause 157	Clause 157	Clause 155
Section 159	Clause 152	Clause 152	Clause 158	Clause 158	Clause 156
Section 160	Clause 153	Clause 153	Clause 159	Clause 159	Clause 157
Section 161			Clause 160	Clause 160	Clause 158
Section 162	Clause 154	Clause 154	Clause 161	Clause 161	Clause 159
Section 163	Clause 155	Clause 155	Clause 162	Clause 162	Clause 160
Section 164					
Section 165	Clause 156	Clause 156	Clause 163	Clause 163	Clause 161
Section 166	Clause 157	Clause 157	Clause 164	Clause 164	Clause 162

Section of the Act	Bill as introduced in the Lords	Bill as amended in Committee in the Lords	Bill as amended on Report in the Lords	Bill as brought from the Lords	Bill as amended in Public Bill Committee in the Commons
Section 167	Clause 158	Clause 158	Clause 165	Clause 165	Clause 163
Section 168	Clause 159	Clause 159	Clause 166	Clause 166	Clause 164
Section 169	Clause 160	Clause 160	Clause 167	Clause 167	Clause 165
Section 170	Clause 161	Clause 161	Clause 170	Clause 170	Clause 166
Section 171	Clause 162	Clause 162	Clause 171	Clause 171	Clause 167
Section 172			Clause 172	Clause 172	Clause 168
Section 173	Clause 163	Clause 163	Clause 173	Clause 173	Clause 169
Section 174	Clause 164	Clause 164	Clause 174	Clause 174	Clause 170
Section 175	Clause 165	Clause 165	Clause 175	Clause 175	Clause 171
Section 176	Clause 166	Clause 166	Clause 176	Clause 176	Clause 172
Section 177					
Section 178					
Section 179					
Section 180	Clause 167	Clause 167	Clause 177	Clause 177	Clause 173
Section 181	Clause 168	Clause 168	Clause 178	Clause 178	Clause 174
Section 182	Clause 169	Clause 169	Clause 179	Clause 179	Clause 175
Section 183	Clause 170	Clause 170	Clause 180	Clause 180	Clause 176
Section 184	Clause 171	Clause 171	Clause 181	Clause 181	Clause 177
Section 185	Clause 172	Clause 172	Clause 182	Clause 182	Clause 178
Section 186	Clause 174	Clause 174	Clause 184	Clause 184	Clause 179
Section 187	Clause 173	Clause 173	Clause 183	Clause 183	Clause 180
Section 188					Clause 181
Section 189					Clause 182
Section 190					
Section 191		Clause 175	Clause 185	Clause 185	Clause 183
Section 192		Clause 176	Clause 186	Clause 186	Clause 184
Section 193		Clause 177	Clause 187	Clause 187	Clause 185
Section 194		Clause 178	Clause 188	Clause 188	Clause 186
Section 195					
Section 196	Clause 175	Clause 179	Clause 189	Clause 189	Clause 187
Section 197	Clause 176	Clause 180	Clause 190	Clause 190	Clause 188
Section 198	Clause 177	Clause 181	Clause 191	Clause 191	Clause 189
Section 199	Clause 178	Clause 182	Clause 192	Clause 192	Clause 190
Section 200	Clause 179	Clause 183	Clause 193	Clause 193	Clause 191

Section of the Act	Bill as introduced in the Lords	Bill as amended in Committee in the Lords	Bill as amended on Report in the Lords	Bill as brought from the Lords	Bill as amended in Public Bill Committee in the Commons
Section 201	Clause 180	Clause 184	Clause 194	Clause 194	Clause 192
Section 202	Clause 181	Clause 185	Clause 195	Clause 195	Clause 193
Section 203	Clause 182	Clause 186	Clause 196	Clause 196	Clause 194
Section 204	Clause 183	Clause 187	Clause 197	Clause 197	Clause 195
Section 205	Clause 184	Clause 188	Clause 198	Clause 198	Clause 196
Section 206	Clause 185	Clause 189	Clause 199	Clause 199	Clause 197
Section 207	Clause 186	Clause 190	Clause 200	Clause 200	Clause 198
Section 208	Clause 187	Clause 191	Clause 201	Clause 201	Clause 199
Section 209	Clause 188	Clause 192	Clause 202	Clause 202	Clause 200
Section 210	Clause 189	Clause 193	Clause 203	Clause 203	Clause 201
Section 211	Clause 190	Clause 194	Clause 204	Clause 204	Clause 202
Section 212	Clause 191	Clause 195	Clause 205	Clause 205	Clause 203
Section 213	Clause 192	Clause 196	Clause 206	Clause 206	Clause 204
Section 214	Clause 193	Clause 197	Clause 207	Clause 207	Clause 205
Section 215	Clause 194	Clause 198	Clause 208	Clause 208	Clause 206
Schedule 1	Schedule 1	Schedule 1	Schedule 1	Schedule 1	Schedule 1
Schedule 2	Schedule 2	Schedule 2	Schedule 2	Schedule 2	Schedule 2
Schedule 3	Schedule 3	Schedule 3	Schedule 3	Schedule 3	Schedule 3
Schedule 4	Schedule 4	Schedule 4	Schedule 4	Schedule 4	Schedule 4
Schedule 5	Schedule 5	Schedule 5	Schedule 5	Schedule 5	Schedule 5
Schedule 6	Schedule 6	Schedule 6	Schedule 6	Schedule 6	Schedule 6
Schedule 7	Schedule 7	Schedule 7	Schedule 7	Schedule 7	Schedule 7
Schedule 8	Schedule 8	Schedule 8	Schedule 8	Schedule 8	Schedule 8
Schedule 9	Schedule 9	Schedule 9	Schedule 9	Schedule 9	Schedule 9
Schedule 10	Schedule 10	Schedule 10	Schedule 10	Schedule 10	Schedule 10
Schedule 11	Schedule 11	Schedule 11	Schedule 11	Schedule 11	Schedule 11
Schedule 12	Schedule 12	Schedule 12	Schedule 12	Schedule 12	Schedule 12
Schedule 13	Schedule 13	Schedule 13	Schedule 13	Schedule 13	Schedule 13
Schedule 14	Schedule 14	Schedule 14	Schedule 14	Schedule 14	Schedule 14
Schedule 15	Schedule 15	Schedule 15	Schedule 15	Schedule 15	Schedule 15
Schedule 16	Schedule 16	Schedule 16	Schedule 16	Schedule 16	Schedule 16
Schedule 17					
Schedule 18	Schedule 17	Schedule 17	Schedule 17	Schedule 17	Schedule 17
Schedule 19	Schedule 18	Schedule 18	Schedule 18	Schedule 18	Schedule 18

Section of the Act	Bill as introduced in the Lords	Bill as amended in Committee in the Lords	Bill as amended on Report in the Lords	Bill as brought from the Lords	Bill as amended in Public Bill Committee in the Commons
Schedule 20					

Annex E – LED Transposition Table

Article	Recital(s)	Copy out (yes/no)	If no – reason for elaboration or non-transposition	Corresponding section
1	1 to 11 and 15	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)).	29 and 31
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 section 29(1) and (2). Article 2(3)(a) has not been transposed as the provisions in Part 3 of the Act 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 Act.	29
3	12, 13, 18, and 21 to 24	In part	The definition of "personal data" in section 3(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, section 3(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). For legal clarity Schedule 7 contains a list of the primary competent authorities to whom Part 3 of the Act applies rather than adopt the definition in Article 3(7). Other competent authorities are caught by section 30(1)(b). 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). 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. Part 3 of the Act 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.	3(2) to (7), 30 to 33, and 205(1) and Schedule 7
4	26 to 30	In part	Section 34 provides an overview of the six data protection principles set out in Article 4(1) and amplified in Articles 5 to 10 In transposing Article 4(4), section 34(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. 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	34, 35(1), 36, 37, 38(1), 39(1), 40, 41, 56 and 57

Article	Recital(s)	Copy out (yes/no)	If no – reason for elaboration or non-transposition	Corresponding section
			indirectly, of data subjects.	
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.	39(2)
6	31	In part	For greater clarity, section 38(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.	38(3)
7	32	Yes	N/A	38(2), (4) and (5)
8	33 to 35	In part	Part 3 of the Act 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.	35(1) and (2)
9	36	No	Section 36(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 Act 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. As the ambit of Articles 9(3) and (4) is unclear, section 80 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.	36 and 80
10	37	Yes	N/A	35(3) to (5) and (8) and Schedule 8
11	38 and 51	Yes	N/A	49 and 50
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. Rather than adopt the qualification in Article 12(1), section 52(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. Section 52(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	44, to 50 and 52 to 53

Article	Recital(s)	Copy out (yes/no)	If no – reason for elaboration or non-transposition	Corresponding section
			confirmed. Article 12(4) enables a controller to charge a reasonable fee where a request from a data subject is manifestly unfounded or excessive; section 53(4) and (5) augments this provision by providing for a power, by regulations, to prescribe a maximum fee.	
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.	44 and 45
14	43	Yes	N/A	45(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.	45(4)-(7)
16	47	In part	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). Section 47(2) therefore requires a controller to restrict processing where data is required for evidential purposes. The additional words in brackets in section 46(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). 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 section 48(7) recognises that there could be cases where there is no competent authority from which the inaccurate personal data originates.	46 to 48
17	48	Yes	N/A	51
18	49	Yes	N/A	43(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.	56
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 "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.	55(3) and 57
21	54	In part	It is not considered necessary to transpose the wording "in	58

Article	Recital(s)	Copy out (yes/no)	If no – reason for elaboration or non-transposition	Corresponding section
			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 section 58(3)) enabling a data subject to exercise his or her rights against any joint controller.	
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".	59
23	50	Yes	N/A	60
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.	61
25	57	In part	Section 62(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.	62
26	59	Yes	N/A	63
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.	64
28	59	In part	Article 28(1) provides the controller or processor must consult the Information Commissioner, in certain cases, prior to processing; section 65(2) places this duty 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).	65
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. Section 66(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).	55(3) and 66
30	61	Yes	N/A	67
31	62	Yes	N/A	68
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.	69
33	63	In part	Section 70(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	70

Article	Recital(s)	Copy out (yes/no)	If no – reason for elaboration or non-transposition	Corresponding section
			data protection officers.	
34	63	In part	Section 71(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.	71
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, section 78(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.	73 and 78
36	66 to 70	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; section 73(3) achieves this without the need for more in section 74.	74
37	71	In part	Section 75(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.	75
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". Section 76(4) adopts the definition of a "legal purpose" in paragraph 5 of Schedule 4 to the 1998 Act.	76
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.	77
40	74 and 83	In part	This Article replicates the GDPR Article 50 which is considered and provided for in Part 5 of the Act.	118(4) and Part 1 of Schedule 14
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 may also discharge the functions of a supervisory authority under the LED. The Act 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).	114, 116(1)(a) and Part 1 of Schedule 14
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 section 128). Provision in respect of conflicts of interest (Article 42(3)) would be included in Commissioner's terms of appointment. Paragraph 5 of	Schedule 12, paragraphs 1(2), 4, 5, 6, 9, 10 and 11

Article	Recital(s)	Copy out (yes/no)	If no – reason for elaboration or non-transposition	Corresponding section
			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)).	
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 long holds that office. Paragraph 3 of Schedule 12 provides for an exhaustive list of grounds for the removal of the Information Commissioner.	Schedule 12, paragraphs 2, 3 and 5
44	77	No	Section 114(1) 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, section 132 provides for an offence of unlawful disclosure by Information Commissioner staff.	114, 132 and Schedule 12, paragraphs 2, 3 and 5
45	80	No	It is not considered necessary to transpose Article 45(1) on the basis that the measures in Part 5 of the Act relating to the functions and powers of the Information Commissioner satisfy the requirements of this provision.	116 and 117
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. Section 134 enables the Commissioner to charge fees to persons other than data subjects and data protection officers.	51, 53, 116, 134, 135, 165, 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.	162, 163, 164, Part 6 and Schedule 13
48	82 and 61	Yes	N/A	81

Article	Recital(s)	Copy out (yes/no)	If no – reason for elaboration or non-transposition	Corresponding section
49	N/A	In part	Section 139 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.	139
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	165
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.	162, 163 and 164
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.	167
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.	187(2) to (4)
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.	169
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.	155 to 159 and Schedule 16
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 2014 Regulations gave effect to Framework Decision 2008/977/JHS – Part 4 of the Regulations is repealed by Schedule 18.	Paragraph 363 of Schedule 19
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 6 May 2016 for cooperation in criminal matters. Domestic provision is not required to give effect to this Article.	N/A
62		No	Article 62 (Article 97 of the GDPR) places a duty of the European	N/A

Article	Recital(s)	Copy out (yes/no)	If no – reason for elaboration or non-transposition	Corresponding section
			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.	
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 May 2018. The provisions of the Act giving effect to the LED will be brought into force by commencement regulations made under section 212(1) and (4). Section 213 enables regulations to make transitional provision as provided for in Article 63(2) and (3).	212 , 213, and paragraph 14 of Schedule 20
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

Printed and published in the UK by The Stationery Office Limited under the authority and superintendence of Jeff James, Controller of Her Majesty's Stationery Office and Queen's Printer of Acts of Parliament.