DATA PROTECTION AND DIGITAL INFORMATION BILL

EXPLANATORY NOTES

What these notes do

These Explanatory Notes relate to the Data Protection and Digital Information Bill as introduced in the House of Commons on 8 November 2023 (Bill 1). A carry over motion was passed in the House of Commons on 17 April 2023.

- These Explanatory Notes have been prepared by the Department for Science, Innovation and Technology, Department for Health and Social Care, the Home Office, Cabinet Office, and the Department for Business and Trade, in order to assist the reader. They do not form part of the Bill and have not been endorsed by Parliament.
- These Explanatory Notes explain what each part of the Bill will mean in practice; provide background information on the development of policy; and provide additional information on how the Bill will affect existing legislation in this area.

- These Explanatory Notes might best be read alongside the Bill. They are not, and are not intended to be, a comprehensive description of the Bill.

Table of Contents

Subject — Page of these Notes

Overview of the Bill

1. This Bill is intended to update and simplify the UK's data protection framework with a view to reducing burdens on organisations while maintaining high data protection standards.
2. The Bill would provide organisations with greater flexibility on how to comply with certain aspects of the data protection legislation; improving the clarity of the framework, particularly for research organisations; and providing more certainty and stability for cross-border flows of personal data. It also extends data sharing powers under section 35 of the Digital Economy Act (DEA) 2017 to include businesses, with a view to better enabling targeted government services to support business growth and to deliver joined-up public services and reduce legal barriers to data sharing.
3. The Bill also contains provisions to reform the regulator, the Information Commissioner, including its governance structure, duties, enforcement powers, reporting requirements, data protection complaints processes and its development of statutory codes of practice.

4. The Bill establishes a framework for the provision of digital verification services in the United Kingdom (UK) to secure the reliability of those services and to enable digital identities and attributes to be used with the same confidence as paper documents. The digital verification services measures make provision for a trust framework of rules concerning the provision of digital verification services, a register of organisations providing digital verification services, a trust mark for use by registered organisations and an information gateway to enable public authorities to disclose personal information to registered organisations for identity and eligibility verification purposes.

5. The provisions on information standards for health and adult social care in England make clear that information standards published under section 250 of the Health and Social Care Act 2012 in relation to the processing of information include standards relating to information technology (IT) or IT services. The provisions extend the persons to whom information standards may apply to include providers of IT, IT services or information processing services using IT used, or intended

for use, in connection with the provision in, or in relation to, England of health or adult social care.

6. The provisions on Smart Data schemes allow for the secure sharing of customer data, e.g., held by a communications provider or financial services provider, upon the customer's request, with authorised third-party providers (ATPs). ATPs, or data intermediaries, use the customer's data to provide innovative services for the consumer or business, such as efficient switching and personalised market comparisons, account management, for example via account aggregation, and cross-sector user-centric control of data.

7. The Bill includes provisions facilitating the flow and use of personal data for law enforcement and national security purposes to enhance the work of law enforcement and national security agencies in the interest of public security.

8. The Bill reforms the way in which births and deaths are registered in England and Wales, enabling the move from a paper-based system to registration in an electronic register.

Policy background

Changes to the Data Protection Act 2018 and UK General Data Protection Regulation

9. It has been over 4 years since the EU General Data Protection Regulations applied to the UK, as supplemented by the Data Protection Act (DPA) 2018. Since then the UK has left the EU. Having reflected on the advantages and disadvantages of the current framework, the government identified and consulted on a number of areas where it considered improvements could be made that would benefit those who process personal data whilst retaining high data protection standards.

10. In the government's view, some elements of current data protection legislation - the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018 - create barriers, uncertainty and unnecessary burdens for businesses and consumers.

11. There is some uncertainty about the different lawful grounds for which private companies can process personal data at the request of public bodies. This can create an

unnecessary burden for private organisations and slows down delivery of public services.

12. The current legislation also prescribes a series of activities and controls which organisations must adopt in order to be considered compliant. This approach, in the government's view, can tend towards a 'box-ticking' compliance regime, rather than one which encourages a proactive and systemic approach.

13. In the government's view, the current legislation does not provide the Information Commissioner (the "Commissioner") with a sufficiently clear framework of objectives and duties in relation to its data protection responsibilities, against which to prioritise its activities and resources, evaluate its performance and be held accountable by its stakeholders. Instead, the Commissioner is obliged to fulfil a long list of tasks, as set out in Article 57 of the UK GDPR, but without a strategic framework to guide its work.

14. This Bill would clarify language in the UK GDPR with a view to helping researchers in their use of personal data. It would allow for

the re-use of personal data for the purpose of longer term research studies.

15. The Bill would streamline the requirements the current legislation places on organisations to demonstrate how they are complying with the legislation. It also amends the exemption which organisations can use to charge a reasonable fee for or refuse to respond to a request from a data subject to where a request is deemed to be ‘vexatious or excessive’. This exemption allows requests made without the intention of accessing personal information to be more easily refused or charged for than the existing threshold of ‘manifestly unfounded or excessive’.

16. The Bill would change to the Privacy and Electronic Communications Regulations 2003, relating to confidentiality of terminal equipment (e.g. cookie rules), unsolicited direct marketing communications (e.g. nuisance calls), and communications security (e.g. network traffic and location data).

17. The Bill seeks to clarify the rules on international transfers and cross-border flows of personal data. International data flows can drive commerce, support research and

innovation, and help people to stay socially connected to one another. This Bill is intended to facilitate international trade by providing a clearer and more stable framework for international transfers of personal data. The reformed regime aims to continue ensuring high standards of protection when people's data is transferred overseas, and the data protection tests will focus on the data protection outcomes provided for data subjects, irrespective of form.

Changes to Part 3 and Part 4 of the Data Protection Act 2018

18. Some of the differences between the regimes under Part 3 of the DPA 2018 (which covers law enforcement processing[1]) and the UK GDPR cause difficulties for competent authorities[2] who process under both

[1] The "law enforcement purposes" are defined under section 31 of the DPA 2018. They are "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."

[2] A competent authority is either a body listed under Schedule 7 of the DPA 2018 (the list includes policing bodies, bodies with investigatory functions, bodies with functions relating to offender management, government departments and other bodies) or a body which has a "statutory function" for one of the law enforcement purposes.

depending on the reason for which they are processing the personal data.

19. This Bill would make changes to Part 3 of the DPA 2018 in order to minimise differences across the regimes by introducing a definition of consent that has the same meaning as in the other regimes; by conferring the ability to create codes of conduct and introducing similar exemptions for legal professional privilege and by protecting national security. All of these provisions currently exist under the UK GDPR.

20. The Bill would also amend Part 3 of the DPA 2018 to remove the requirement for competent authorities to inform the data subject that they have been subject to automated decision-making if certain conditions are met. This change reflects the fact that, under certain circumstances, the current requirement could risk prejudicing an active investigation by tipping off an individual that they are of interest to the police.

21. The Bill would also amend the requirement for controllers to keep logs relating to processing, removing the requirement to record a justification in the logs of consultation

and disclosure, which is often resource intensive and holds limited value in maintaining accountability as it is unlikely that someone wrongly accessing would enter an honest justification. The other safeguards, such as recording the time and date, will remain in legislation.

22. The current situation where law enforcement bodies and the intelligence services are governed by different data protection regimes presents challenges to joint operational working. In response to the Manchester and Fishmongers' Hall terrorist incidents and the increasing expectation that Law Enforcement and the Intelligence Services will work jointly in operational partnerships, the Bill would introduce a power that will allow the Secretary of State to issue a notice designating some specified competent authorities to process data jointly with the Intelligence Services under Part 4 of the DPA 2018 for national security purposes. This is intended to enable these operational partnerships to respond to national security threats and protect the public, particularly where the processing of data requires complex decisions at pace.

Implementation of law enforcement information-sharing agreements

23. This Bill would enable swift implementation of new international law enforcement information-sharing agreements, thereby providing UK law enforcement agencies with additional capabilities at the earliest point possible. These new agreements will set the parameters for the sharing of law enforcement data between the UK and a third country, including the technical specifications relating to how data will be shared.

24. One example envisaged in relation to new international law enforcement information sharing agreements, is an agreement enabling a data sharing process where international partners' relevant authorities searching a UK 'alert store' containing bilateral alerts. Frontline officers in the UK's police forces, NCA, and border forces would have a similar ability to search the platforms of international partners and access relevant data.

25. The regulation making power provided under this clause will allow the appropriate national authority to make regulations to implement the technical and, where

appropriate operational detail, of any such international agreements.

Changes to oversight of police use of biometrics and surveillance cameras

26. In the government's view, the current oversight arrangements for police use of biometrics and surveillance cameras to help identify and eliminate suspects are complex and confusing for the police (as controllers) and the wider public. The Protection of Freedoms Act 2012 (POFA) introduced two independent commissioners to oversee police use of biometrics (the Commissioner for the Retention and Use of Biometric Material the "Biometrics Commissioner") and police and local authority use of overt surveillance cameras (the Surveillance Camera Commissioner), and a Surveillance Camera Code of Practice. Under the DPA 2018, the Information Commissioner provides independent oversight of all controllers' use of all personal data. This includes the use of biometrics and surveillance cameras.

27. The Information Commissioner has extensive regulatory powers and issues its own guidance to controllers including the

police, which is published. As a result of this overlap, the government consulted on simplifying these arrangements.

28. This Bill would simplify the oversight framework for the police use of biometrics and police and local authority use of surveillance cameras. It would abolish the Biometrics and Surveillance Camera Commissioners' posts, and the Surveillance Camera Code. The Information Commissioner's Office, which covers the use of all personal data by all bodies, remains in place. The Bill would transfer these review functions to the Investigatory Powers Commissioner. The Bill would also update the scope of the police National DNA Database Board to reflect its similar oversight of the police national fingerprint database and provide the Secretary of State with a power by affirmative regulations to amend the scope of this Board.

Registers of births and deaths

29. The birth of every child in England and Wales is required to be registered by the registrar of births and deaths for the sub-district in which the child was born. Similarly, the death of every person dying in England or

Wales is required to be registered by the registrar of births and deaths for the sub-district in which the death occurred.

30. This Bill would remove the requirement for paper registers to be held and stored securely in each registration district and enable all births and deaths to be registered electronically. This will remove the current duplication whereby births and deaths are registered both electronically and in paper registers.

31. Births and deaths will continue to be registered on information provided by a qualified informant at the register office in the sub-district in which the birth or death occurred. The Bill includes a regulation-making power for the relevant minister to make regulations, to provide that if a person complies with specified requirements at the time of registering a birth or death they are to be treated as having signed the register in the presence of the registrar. This may include requiring a person to sign something other than the register or requiring a person to provide specified evidence of identity.

32. With the introduction of an electronic register there will no longer be a requirement

for the system of quarterly returns, as all birth and death entries will be held on the single electronic register maintained by the Registrar General.

Digital Verification Services

33. There is currently no existing legislation relating to the regulation of private organisations providing digital verification services in the UK. The digital verification service provisions in this Bill aim to increase trust in and acceptance of digital identities across the UK to help make identity proofing easier, cheaper and more secure and to enable a trusted digital identity market to develop in the UK for those that choose to use it to prove things about themselves, for example when starting a new job or moving house. To do this, the Bill would establish a regulatory framework for the provision of digital verification services in the UK and enable public authorities to disclose personal information to trusted digital verification services providers for the purpose of identity and eligibility verification.

Extending data sharing powers under section 35 of the Digital Economy Act 2017

34. For public service delivery, the existing power under section 35 of the Digital Economy Act (DEA) 2017 allows for data sharing that benefits households and individuals. To facilitate more responsive, joined-up public services across the digital economy, this Bill extends powers under section 35 to allow data sharing to deliver public services to businesses.

35. Extending the powers enables businesses to access government services and support more easily, giving them easier access to information, guidance and business support services.

Health and Adult Social Care System

36. For the health and adult social care system to work efficiently and effectively, data needs to flow through the system in a standardised way, so that when it is accessed by or provided to an organisation for any purpose it can be read, be meaningful to, and be easily

understood by the recipient and/or user of the data. This relies on data being collected, processed, and shared in a consistent way.

37. This Bill would support appropriate data-sharing across the wider health and adult social care sector.

38. Information standards set standards relating to processing information, including standards about how information is shared, and which make it easier to compare data, across the health and adult social care sector. They are prepared and published by the Secretary of State (in relation to health care and adult social care) and by NHS England (in relation to NHS services). They apply to the Secretary of State and NHS England, public bodies which exercise functions in connection with the provision of health or adult social care and providers of such care who are required to be registered with the Care Quality Commission.

Smart Data schemes

39. Smart Data is the secure sharing of customer data, upon the customer's request, with authorised third-party providers (ATPs). ATPs can typically be defined as organisations

who are neither the customer nor original service provider (e.g., the bank), and are offering services to the customer.

40. ATPs use the customer's data to provide innovative services for the consumer or business, such as automatic switching and account management, for example via account aggregation. The incumbent industry (e.g., the service provider such as bank) may also opt to innovate and offer similar services.

41. The provisions in this Bill on Smart Data would improve data portability between suppliers, service providers, customers, and relevant third parties with a view to:

- rebalancing the information asymmetry between suppliers and customers;[3]
- enabling customers to make better use of their personal data, e.g., enabling accurate tariff comparisons and providing access to better deals;
- enabling customers to benefit from a more competitive marketplace, including through

[3] Suppliers and service providers collect and store a significant amount of customer data; this data is not typically easily available or accessible in a way that is easy to understand, e.g., in a standardised format.

lower prices and higher quality goods and service delivery;

- provide new services in and across the sectors, such as those which may help consumers save and manage their money and services.

42. Open Banking is a live example of Smart Data. In 2017, following a market investigation due to competition concerns, the CMA ordered the nine biggest banks in the UK to 'open up' the data relating to personal and business current accounts. The CMA set up the Open Banking Implementation Entity to oversee the scheme. As of February 2023, there are over 5 million consumers and small businesses using Open Banking.

Consultations

National Data Strategy and 'Data: A New Direction' consultation

43. At the end of 2020, the UK government launched its National Data Strategy. It outlined the government's view that personal data is a huge strategic asset and the driving force of the world's modern economies, and its view that personal data fuels innovation in

businesses, both large and small, drives scientific discovery and was important during the global coronavirus pandemic.

44. In September 2021 the government launched the “Data: a new direction” consultation to hear views on how it could build on the elements of the current UK GDPR, such as its data processing principles, its data rights for citizens, and its mechanisms for supervision and enforcement.

45. The consultation closed in November 2021 having received close to 3000 responses. These were received from individuals, businesses, and a wide range of organisations including global think tanks, non-profit organisations, research institutes and trade bodies.

46. The government response to the consultation was published on 17 June 2022.

47. The proposals in the response were arranged into 30 headings across 5 chapters:

- chapter one related to providing clarity and certainty to businesses on the interpretation of current laws, definitions

and requirements relating to personal data processing;

- chapter two related to reducing burdens on businesses and delivering better outcomes for people in relation to the processing of personal data;
- chapter three related to trade and barriers to personal data flows;
- chapter four related to delivering public services through use of and access to personal data;
- chapter five related to the reform of the Information Commissioner, the UK's independent data protection regulator.

Digital identity and attributes consultation

48. In July 2021 the government published a Digital identity and attributes consultation. This followed on from the commitments made in the digital identity call for evidence response published in 2020, and the draft UK digital identity and attributes trust framework alpha version 1 published in February 2021.

49. The 2021 consultation sought views on proposals which looked to enable the growth of

a secure and trusted digital identity market in the UK. The proposals included establishing governance to make sure organisations wanting to operate in the digital identity marketplace are supported when they choose to follow the rules and standards set out in the trust framework, and making it possible for more trusted data sets to be checked so people can more easily prove things about themselves as they create a digital identity.

50. The consultation closed in September 2021 and received 270 responses. This consisted of 92 responses from organisations and 178 responses from individuals. The government response to the consultation was published on 10 March 2022.

Smart Data schemes

51. In 2018, the government consulted[4] on whether and how to extend the benefits of Smart Data to sectors beyond retail banking (delivered through Open Banking). Consultation responses were received from the technology, energy, communications, and

[4] BEIS, *Smart Data Review*, 2018

financial sectors, as well as charities and academia.

52. Respondents were in favour of the extension of Smart Data and generally in favour of legislation to mandate industry involvement in Smart Data initiatives, though some wanted more time for voluntary approaches to develop first. No significant voluntary schemes have developed in the absence of effective legislation and regulations.

53. The government's consultation response committed to primary legislation to extend the government's powers to mandate participation in Smart Data initiatives, when Parliamentary time allows. [5]

54. The government considered that a voluntary approach would lead to continued slow progress and possible duplication of work across sectors. Delays would stem from limited incentives for data holders to share data; this has been evidenced in the slow progress of similar voluntary schemes, such as the Data Transfer Project and Open Transport. As companies in scope of the schemes are likely

[5] BEIS, *Smart Data: putting customers in control of their data and enabling innovation, 2019*

to bear much of the cost of Smart Data, there is a high risk that no schemes will voluntarily emerge on a wide scale.

Legal background

Data Protection

55. The UK is a party to the Council of Europe "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", which became open for signature in 1981. Parliament passed the Data Protection Act 1984 to ensure compliance with the standards set out in the Convention and ratified the Convention in 1985.

56. The Data Protection Act 1984 was repealed and replaced by the Data Protection Act 1998, which implemented the EU Data Protection Directive (95/46/EC) (“the 1995 Directive”).

57. The 1995 Directive was replaced by the EU General Data Protection Regulation (2016/679) (the "EU GDPR"), which applied directly in the UK from 25 May 2018. This was supplemented in the UK by the Data Protection Act 2018 ("DPA 2018") (in particular in Part 2 of the Act), which repealed the Data Protection Act 1998 and exercised derogations provided by the EU GDPR.

58. The EU GDPR does not apply to processing by competent authorities for law enforcement purposes. Such processing is subject to EU Directive 2016/680, which was transposed into UK law in DPA 2018 (in particular in Part 3 of the Act).

59. The DPA 2018 provides for a further processing regime for processing by the Intelligence Services (in Part 4 of the Act).

60. The EU GDPR was incorporated into UK law at the end of the EU Transition Period under section 3 of the European Union (Withdrawal) Act 2018 (EUWA 2018) and modified by the Data Protection, Privacy and Electronic Communication (Amendments etc) (EU Exit) Regulations 2019 under the power in section 8 EUWA 2018 to create the UK GDPR.

61. The UK's data protection framework therefore comprises three regulatory regimes:

- general processing of personal data - governed by the UK GDPR as supplemented by Part 2 of the Data Protection Act 2018;
- processing by "competent authorities" (as defined in section 30 & schedule 7 DPA 2018) for law enforcement purposes - governed by Part 3 DPA 2018, which implemented EU Directive 2016/680 (the EU Law Enforcement Directive) into UK law;
- processing by the UK intelligence services - governed by Part 4 DPA 2018.

62. The Privacy and Electronic Communications (EC Directive) Regulations 2003 transposed Directive 2022/58/EC. These contain some special rules for certain types of processing, such as personal data collected through cookies and direct marketing, which overlay the general rules for processing in the UK GDPR.

63. The Data Protection and Digital Information Bill makes various amendments to these existing sources of data protection law.

Implementation of law enforcement information-sharing agreements

64. It is envisaged that under future international agreements law enforcement information will be shared between UK law enforcement agencies, particularly, police forces, the National Crime Agency and Border Force and equivalent organisations in the relevant third countries. The data will likely be shared using a new IT platform.

65. UK police forces, the NCA and Border Force already have the ability to share law enforcement data with international partners, using their existing statutory or common law powers.

66. The government's view is that new domestic legislation is now required, since:

- the UK will need to create secondary legislation with sufficient detail to enable each agreement's implementation;
- operational partners (such as police) will, if they have legislation to follow, be more explicitly aware of their obligations,

providing legal assurance that the risk of non-compliance has been mitigated;

- international partners are likely to require or prefer that agreements have a basis in UK legislation, not in common law, as the common law is not a familiar concept to some.

Police use of biometrics

67. The Bill would simplify the oversight framework for the police use of biometrics and police and local authority use of surveillance cameras. It would abolish the Biometrics and Surveillance Camera Commissioners' posts, and the Surveillance Camera Code. The Bill would also update the name and scope of the police National DNA Database Board to reflect its similar oversight of the police national fingerprint database (IDENT1) and provide powers for the Secretary of State to make changes to the name and scope of this board.

Registers of births and deaths

68. The provision for registering births and deaths is principally governed by the Births and Deaths Registration Act 1953, the Registration Service Act 1953 and the

Registration of Births and Deaths Regulations 1987 which are based on legislation that has been in place since 1836.

Digital Verification Services

69. The current legal framework on data sharing means that there are sometimes restrictions on the ability of public authorities to share information with private organisations for the purposes of providing digital verification services. The new powers in the Bill would enable public authorities to share information subject to safeguards that help to protect personal information.

Extending data sharing powers under section 35 of the Digital Economy Act 2017

70. The sharing of information held by different public bodies can help those bodies deliver better public services. The DEA 2017 allows data sharing in order to deliver public services which benefit individuals and households. Clause 92 of this Bill amends section 35 to extend these data sharing powers to support

the delivery of public services which benefit businesses, or “undertakings”.

71. The clause also defines the term “undertakings” to include those carrying on trade whether for profit or not for profit and any body established for charitable purposes.

72. Part 5 of the DEA 2017, which includes section 35, contains safeguards to limit the circumstances under which information can be shared. Section 35 of the DEA 2017 provides a gateway to enable specified public authorities, listed in Schedule 4 of the DEA 2017, to share information for tightly constrained objectives which must be for the benefit of individuals or households. Those objectives must be set out in regulations and must be for the improvement or targeting of the provision of a public service. The same framework of constraints will apply to the sharing of information to improve delivery of public services to undertakings.

Health and Adult Social Care System

73. Existing legislation regarding the processing of information and IT systems is not sufficient to achieve the policy objective.

Even if existing legislative mechanisms were used to oblige health and adult social care providers to purchase information technology products and services with appropriate technical features (either directly or via professional regulation), this would be insufficient to bring the wholesale change to the supplier market that is needed. This is because the legislation does not concern the providers of the IT on which the processing relies and who can ensure that all IT and services supplied meet relevant technical requirements.

74. In relation to processing of information, the key legislation is section 250 of the Health and Social Care Act 2012 (HSCA 2012) as amended by the Health and Care Act 2022 (HCA 2022). As amended, section 250 will enable the Secretary of State to prepare and publish standards ("information standards") in relation to the processing of information concerning or connected with the provision of health care and adult social care and will enable NHS England to prepare and publish information standards in relation to information concerning or connected with the provision of NHS Services. The standards may be applied

to the Secretary of State, NHS England, public bodies which exercise functions in connection with the provision of health or adult social care and private bodies which are required to be registered with the Care Quality Commission. Where an information standard is applied to a person, that person must comply with the standard, except that the Secretary of State is required only to have regard to an information standard published by NHS England.

75. Section 267 HSCA 2012 confers power on the Secretary of State to establish and operate a scheme for the accreditation of information service providers, which are persons other than public bodies providing services involving the collection, analysis, publication or other dissemination of information in connection with the provision of health services or of adult social care in England. The provision allows the Secretary of State to set criteria to be met by service providers in order to be accredited. This does not allow for establishing and operating an accreditation scheme to accredit IT products and services supplied to the health and adult social care sector.

76. There are also two regulatory powers that could potentially allow for the imposition of

standards on providers of health and adult social care. The first is chapter 3, part 3 HSCA 2012 which allows NHS England to set licence conditions on health service providers required to have a licence such as NHS Foundation Trusts. The Secretary of State may prescribe the purposes for which NHS England can set the licence conditions, the scope of which is considered to be wide enough for conditions to be imposed relating to technical standards for computer systems. The second is section 20 of the Health and Social Care Act 2008 (HSCA 2008) which allows the Secretary of State, by regulations, to impose requirements in relation to regulated activities that providers who are registered with the Care Quality Commission must meet. Current regulations include requirements to establish systems and processes that ensure records relating to service users are secure, accurate, complete and contemporaneous. The HSCA 2008 also confers a function on the Care Quality Commission to monitor the practice followed by registered providers in relation to the processing of information.

Smart Data schemes

77. The clauses in Part 3 contain regulation-making powers and ancillary provisions to allow the Secretary of State or the Treasury, by regulations, to require suppliers of goods, services and digital content specified in the regulations, and other persons who process the relevant data, to provide customers or their authorised representatives with access to data relating to that customer (customer data) and contextual information relating to the goods, services or digital content provided by the supplier (business data). These clauses follow a government commitment, made further to a public consultation in 2019, to obtain powers to introduce “Smart Data schemes” in markets across the economy. Smart Data schemes intend to enable the secure sharing of data, at the customer’s request, with authorised third parties.

78. The objective of these powers, where they are exercised, is to provide enhanced data portability rights beyond the right to data portability in Article 20 of the UK GDPR. The government’s view is that the UK GDPR does not guarantee provision of customer data in “real time” or in a useful format, does not cover wider contextual data and does not apply

where the customer is not an individual.

79. Much (but not all) of the data to which Smart Data schemes will apply will constitute “personal data” to which the UK GDPR applies. The regulation-making powers and regulations are not intended to modify or restrict the application of data protection legislation but rather to provide enhanced data portability beyond the existing regime.

80. These powers will replace the regulation-making powers in section 89-91 (supply of customer data) of the Enterprise and Regulatory Reform Act 2013 (ERRA 2013) which enable the Secretary of State to make regulations to require the suppliers of goods or services to provide customer data to a customer or to a person authorised by the customer at the customer’s or authorised person’s request. The ERRA 2013 powers were introduced as a backstop should it not be possible for suppliers to develop voluntary programmes for the release of customer data.

81. The ERRA 2013 powers are no longer sufficient to enable effective Smart Data schemes. For instance, they do not cover wider business data; they do not allow the

regulations to make provision by reference to specifications and technical requirements published by a specified person which is essential as IT and security standards will require frequent updating to function in a fast-paced IT environment; they do not contain powers to require the collection and retention of data which is necessary to ensure that suppliers have consistent data sets for disclosure; they do not contain powers to regulate the onward disclosure or use of data which might be necessary.

82. Since 2013, the government's understanding of what is required for a successful "Smart Data scheme" has evolved in particular because of the open banking scheme, in which the Competition and Markets Authority, following a market study, ordered (under its competition powers) the nine biggest banks in the UK to open up data relating to personal and business current accounts. The open banking scheme enables customers to share their bank and credit card transaction data securely with third parties who can provide them with applications and services. As of February 2023, there are over 5 million consumers and small businesses using open

banking.

83. The government has also had regard to the recent enactment of powers in Part 4 of the Pension Schemes Act 2021 (which amend the Pensions Act 2004 and the Financial Services and Markets Act 2002) for pensions dashboards, an electronic communications service which allows individuals to access information about their pensions in one place.

Territorial extent and application

84. Clause 118 sets out the territorial extent of the Bill, that is the jurisdictions which the Bill forms part of the law of. The extent of a Bill can be different from its application. Application is about where a Bill produces a practical effect. The territorial extent and application for measures in the Bill are summarised below.

85. See the table in Annex A for a summary of the position regarding territorial extent and application in the UK.

Data protection

86. The Bill's data protection reforms extend to the whole of the UK, apart from one provision relating to the Information Commission's seal, which does not extend to Scotland. The data protection legislation amended by this Bill applies to data controllers and data processors established in the UK, and those processing on their behalf, and there is some extra-territorial application for certain processing of personal data by controllers and processors established in third countries.

Privacy and Electronic Communications Regulations

87. Data protection is a reserved area. The telecommunications reservations in relation to Scotland, Wales and Northern Ireland apply to changes to the Privacy and Electronic Communications (EC Directive) Regulations 2003. No Legislative Consent Motion (LCM) is required.

Changes to Part 3 and Part 4 of DPA 2018

88. Part 3 of the DPA 2018 applies only to processing for law enforcement purposes by competent authorities (defined in s.30 DPA 2018[6]) and those processing on their behalf. Part 4 of the DPA 2018 applies only to the intelligence services (defined in section 82(2)), and those processing on their behalf. Amendments made by this legislation will enable a Secretary of State to permit some competent authorities to also operate under Part 4 in specific circumstances. Data protection is a reserved area, so a LCM is not needed for the provisions related to Parts 3 and 4 of the DPA 2018.

[6] These are either bodies set out under Schedule 7 of the DPA 2018 or other bodies which have a statutory function for any of the law enforcement purposes.

Police use of biometrics

89. Changes to police use of biometrics and overt surveillance are limited to England and Wales[7]. Policing is devolved in Scotland and Northern Ireland, but not in Wales, therefore the Police and Criminal Evidence Act 1984 (which this Bill amends) applies to police forces in England and Wales only – Scotland and Northern Ireland have their own equivalent Acts. No LCM is required.

Implementation of law enforcement information-sharing agreements

90. The territorial extent of these provisions is UK wide. International agreements are reserved by the government as prerogative powers to be excised by the Secretary of State.

91. Whilst international relations are a reserved matter, the domestic implementation of such agreements is devolved, and law enforcement is a devolved matter to varying extents in each devolved administration. This clause provides the appropriate national

[7] The only exception to this is the changes to the oversight of National Security Determinations (applications submitted under s63M of PACE) which will apply UK wide as national security matters are reserved.

authority with the power to make regulations to implement the technical and, where appropriate operational detail, of any such international agreements.

92. The “appropriate national authority”, is defined in clause 100 as, the Secretary of State, Scottish Ministers, and Welsh Ministers, are also appropriate national authorities in relation to regulations under clause 99 which would be within the legislative competence of the Scottish Parliament or Senedd Cymru, respectively. A concurrent power to make regulations has not been included for Northern Ireland, as presently there is not a functioning Executive, and the Assembly is not sitting. It has been agreed the Secretary of State will make regulations relating to Northern Ireland.

93. As a result, a LCM will be required from Scotland, Wales and Northern Ireland.

Registers of Births and Deaths

94. Legislative competence for births and deaths (and civil registration generally) is devolved to Scotland and Northern Ireland and separate legislation exists to govern the

registration of births and deaths in those jurisdictions. Legislative competence in respect of civil registration is not devolved in Wales.

95. The clauses which amend the Births and Deaths Registration Act 1953 and the Registration Service Act 1953, relating to the registration of births and deaths in England and Wales extend and apply to England and Wales only.

96. These provisions also give effect to minor and consequential amendments which do not change the application of the law in Scotland and Northern Ireland, but the provisions amended extend to to Scotland and Northern Ireland. No LCM is required.

97. Provisions in the Bill which enable regulations to make amendments to primary and secondary legislation in consequence of the changes made to birth and death registration in England and Wales extend to the whole of the UK.

Digital Verification Services

98. The territorial extent of these provisions is UK wide. The legislation applies to digital

verification service providers established in the UK.

99. These clauses regulate the provision of digital verification services through the creation of a trust framework, a register of providers, an information gateway, and a trust mark. The provision of digital verification services will be online, though they can be used by individuals across the UK online as well as in person.

100. The reservation of internet services applies in Northern Ireland, Wales and Scotland. No LCM is required.

Extending data sharing powers under section 35 of the Digital Economy Act 2017

101. The territorial extent and application of these provisions is UK wide. Like section 35 of the DEA 2017 , this provision will extend and apply to the UK (though the powers in Part 5, chapter 1 of the DEA 2017 have yet to be commenced in Northern Ireland).

102. There is no relevant reservation for the power in this provision so a LCM is required. The clause relates to public service delivery to businesses which is not solely for reserved purposes but also for devolved purposes, such

as providing devolved public services to businesses. The clause will also alter the executive competence of the Devolved Administrations by extending the scope of their regulation-making powers. It will do this by widening the conditions with which an objective must comply in order to meet the definition of an information-sharing "specified objective" to improve public service delivery under section 35 (9) – (12) of the DEA 2017 by adding public service delivered to businesses.

103. Currently, under s44 and s45 of the DEA 2017, the "appropriate national authority" in relation to the information-sharing powers under section 35 (which is either the Minister for Cabinet Office, Scottish Ministers, Welsh Ministers or Department of Finance in Northern Ireland) may specify an objective under section 35 which relates to individuals and households (where the relevant conditions under section 35 (9) – (12) are met).

104. This provision will allow the "appropriate national authority" to also specify objectives in relation to businesses (where the relevant conditions under section 35 (9) – (12) are met). Devolved Administrations will therefore have new powers, via regulations, to specify new

business-related “specified objectives” to be listed in Schedule 4 of the DEA 2017 and specify which bodies are listed in Schedule 4 of the DEA 2017 as “specified persons” having the power to share information under the “specified objectives”.

Health and Adult Social Care System

105. The territorial extent of these provisions is England and Wales only. The legislation applies to persons involved in marketing, supplying, providing or otherwise making available information technology, an information technology service or an information processing service using information technology in so far as it is used or intended for use in connection with the provision in, or in relation to, England of health care or adult social care. No LCM is required.

Smart Data Schemes

106. The territorial extent of these provisions is UK wide. The legislation applies to businesses operating in the UK.

107. While many aspects of the proposals are reserved, some areas are devolved (e.g. where the customer is a business and not an individual), and consumer protection in Northern Ireland. Therefore a LCM is required in all three Devolved Administrations.

Commentary on provisions of Bill/Act

Part 1: Data Protection

Definition

Clause 1: Information relating to an identifiable living individual

108. The UK GDPR and the DPA 2018 apply to the processing of personal data, which is defined in section 3 of the DPA 2018 as any information relating to an identified or identifiable living individual. The legislation does not apply to non-personal or anonymous data, so the purpose of this clause is to provide greater clarity about which type of data is in scope of the legislation.

109. Clause 1 (1) amends section 3(3) of the DPA 2018 by confirming that a living individual may be identifiable either directly or indirectly.

110. Clause 1 (2) adds new section 3A to the DPA 2018. New section 3A(1)-(3) set out two cases in which information being processed by a controller or processor counts as information relating to an identifiable individual and is therefore personal data for the purposes of the legislation.

111. The first case is where the controller or processor can themselves identify a living individual from the information they are processing by reasonable means. The second case is where the controller or processor knows or ought reasonably to know that another person is likely to obtain the information as a result of the processing - for example, somebody with whom the information is shared - could identify a living individual by reasonable means.

112. New section 3A (4) clarifies that “obtaining information as a result of the processing” as referenced in subsection 3A(3)(a) also includes information being obtained as a result of inaction by the controller or processor; eg. as a result of their failure to put in place appropriate measures to prevent, or reduce the risk of, hacking.

113. New section 3A(5) and (6) elaborate on the meaning of “by reasonable means”. This includes any means that the controller is likely to use, taking account of, amongst other things, the time, effort and cost to identify an individual from the information. The technology that is available to the person or organisation that is processing the information is also likely

to be a relevant factor. The list of considerations which may be relevant is not exhaustive. Other factors, such as whether steps taken to identify or re-identify data subjects would be lawful and or proportionate in a particular situation may be relevant to the overall assessment of reasonableness.

114. Clause 1 (3) makes some changes to the definitions in Article 4 of the UK GDPR to make sure the language on identifiable living individuals and the meaning of pseudonymisation is consistent with terms in section 3 of the DPA 2018.

115. Clause 1 (4) makes minor amendments to section 6 of the DPA 2018, which are consequential to the changes to Article 4 of the UK GDPR made by clause 1 (3).

Clause 2: Meaning of research and statistical purposes

116. Clause 2 amends Article 4 of the UK GDPR. Clause 2 (1) inserts a definition of what constitutes processing for scientific research under the UK GDPR into new paragraphs 3 and 4 of Article 4. Only processing that could

reasonably be described as scientific research can fall under this definition. Provided that the processing meets this requirement, it does not matter whether the research is privately or publicly funded or whether it was carried out as a commercial or non-commercial activity.

117. New Article 4(4)(a) gives examples of the types of scientific research that could fall under the definition, provided that they meet the requirement referenced above. This list provides examples of types of scientific research, such as applied or fundamental research or innovative research into technological development. However, this list is non-exhaustive and scientific research is not restricted to exclusively these types.

118. New Article 4(4)(b) clarifies that research into public health only falls under the definition of scientific research if it is in the public interest.

119. Clause 2 also inserts a new paragraph 5 of Article 4 which clarifies that processing for genealogical research is to be considered as processing for historical research under the UK GDPR.

120. Clause 2 also inserts a definition of what

constitutes processing for statistical purposes under the UK GDPR into the new paragraph 6 of Article 4, along with two conditions in order to meet the definition.

Clause 3: Consent to processing for the purposes of scientific research

121. Clause 3 amends Article 4 of the UK GDPR by clarifying a way for data controllers processing for scientific research purposes to obtain consent to an area of scientific research where it is not possible to identify fully the purposes for which the personal data is to be processed at the time of collection. Clause 3 clarifies when consent in such cases will meet the existing definition under the UK GDPR which must satisfy the conditions found in new Article 4(7)(a)-(d).

Clause 4: Consent to law enforcement processing

122. Clause 4 introduces a definition of consent into Part 3 of the DPA 2018.

123. Consent should only be used as the grounds for processing where it would be inappropriate to use one of the law enforcement purposes.

124. For consent to be a valid ground for processing it must be freely given, informed and an unambiguous indication of the data subject's wishes. A lack of response by the data subject, or the use of pre-ticked boxes, cannot be understood to indicate consent by the data subject. Where processing has multiple purposes, consent must be given for each of them.

125. If the data subject is unable to withdraw their consent without suffering a negative consequence, it cannot be regarded as freely given and should not be used as the legal basis for processing.

126. Where competent authorities rely upon consent to process personal data, they should be able to demonstrate that this has been freely given by the data subject in a clear, comprehensible and easily accessible manner. Pre-written declarations of consent by the controller must use clear and understandable language.

127. When using consent, competent authorities must at least make the data subject aware of the identity of the competent authority and their purposes for processing.

Data protection principles

Clause 5: Lawfulness of processing

128. Clause 5 amends Article 6 of the UK GDPR which is concerned with the lawful grounds for processing personal data. The clause makes some clarifications to the public tasks lawful ground in Article 6(1)(e) and introduces a new lawful ground under new Article 6(1)(ea). It also sets out examples of activities which may be in the legitimate interest of the data controller when relying on Article 6(1)(f).

129. Article 6(1)(e) UK GDPR provides a lawful basis for processing 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. Subsection (2)(a) makes it clear that the task carried out in the public interest referred to in A6(1)(e) must be that of the controller. This means that a controller cannot process personal data in reliance on another controller's tasks carried out in the public interest under A6(1)(e). Section 8 of the Data Protection Act 2018 and regulation 41(2) of the The Money Laundering, Terrorist Financing and Transfer of Funds

(Information on the Payer) Regulations 2017 provide additional clarity on the sorts of activities that constitute tasks carried out in the public interest for the purposes of Article 6(1)(e). These should be read consistently with these changes so that tasks arising from the activities are read as being those of the relevant controller.

130. Subsection (2)(b) creates a new lawful ground for processing personal data by inserting new Article 6(1)(ea) into the UK GDPR. New Article 6(1)(ea) provides that processing will be lawful where it is necessary for a recognised legitimate interest.

131. Subsection (2)(c) amends Article 6(1) UK GDPR to prevent new Article 6(1)(ea) from being relied on by public authorities in the performance of their tasks, consistent with the existing restriction in respect of Article 6(1)(f). This means that new Article 6(1)(ea) will only be available to controllers that are not public authorities or where public authorities are not processing personal data in the performance of their tasks.

132. Subsection (3) mirrors the amendments made by subsection (2)(a) by similarly

restricting references to “tasks” in Article 6(3) UK GDPR to those of the controller.

133. Subsection (4) inserts new paragraphs into Article 6 UK GDPR. New Article 6(5) defines processing necessary for a recognised legitimate interest for the purposes of new Article 6(1)(ea) as being processing that meets a condition in new Annex 1 to the UK GDPR (inserted by subsection (7) and Schedule 1). Under new Article 6(6) to (8) the Secretary of State may make regulations to add to, vary or (in certain cases) omit recognised legitimate interest activities in Annex 1. Before laying regulations, the Secretary of State must have regard to the effects of any changes on the interests and fundamental rights and freedoms of data subjects, particularly children. The regulations must be made by statutory instrument and are subject to the affirmative procedure.

134. Subsection (5) ensures that the right to object in Article 21 UK GDPR applies to new Article 6(1)(ea).

135. Subsection (7) makes amendments to section 8 of the Data Protection Act 2018, including the removal of section 8(e) (an

activity that supports or promotes democratic engagement). This activity has been removed from section 8 as it has been included in new Annex 1 to the UK GDPR (inserted by Schedule 1) as a recognised legitimate interest.

136. Subsection (9) sets out examples of activities which may constitute legitimate interests for the purposes of Article 6(1)(f) of the UK GDPR. Processing of personal data for these activities must be necessary and the data controller is required to make sure that its interests in processing the data without consent are not outweighed by the individual's rights and interests. The examples given in subsection (9) are illustrative only and non-exhaustive. Data controllers may rely on Article 6(1)(f) to process personal data for other legitimate activities, providing the processing is necessary for the activity and appropriate consideration is given to the potential impact of the processing on the rights and interests of data subjects.

137. Subsection (10) defines the meaning of "intra-group transmission" and "security of network and information systems", expressions used in subsection (9).

Clause 6: The purpose limitation

138. Clause 6 sets out the conditions for determining whether the reuse of personal data (otherwise known as "further processing") is permitted in compliance with the purpose limitation principle outlined in Article 5(1)(b) of the UK GDPR. This principle prohibits further processing that is not compatible with the original purpose for which the personal data was collected.

139. The conditions are made by way of a series of amendments to the UK GDPR (subsection (1)).

140. Subsection(2) amends Article 5(1)(b) of the UK GDPR in order to clarify that the rules around further processing apply to personal data collected from a data subject or otherwise by the controller or a processor currently processing that data. The rules do not apply where there has been a change of controller.

141. Subsection(3) clarifies that meeting a condition under Article 8A for further processing does not permit controllers to continue relying on the same lawful basis under Article 6(1) that they relied on for their original purpose if that basis is no longer valid for the new purpose. In many cases, controllers will be able to establish a lawful basis under Article 6(1) for the new purpose through satisfying the conditions under the new Article 8A.

142. Subsection(4) removes Article 6(4) from the UK GDPR, since the provisions for further processing have now been set out in the new Article 8A.

143. Subsection(5) inserts a new Article 8A into the UK GDPR in order to set out the conditions under which further processing of personal data complies with the purpose limitation principle in Article 5(1)(b) of the UK GDPR.

144. New Article 8A(2) sets out considerations required in order for a person to be able to evaluate whether their processing is compatible with the original purpose. Factors to be taken into account in the evaluation

include any link with the original processing and the effects on the data subject.

145. New Article 8A(3) lists the circumstances in which a purpose is to be treated as compatible with the controller's original purpose. If one of these circumstances applies, the controller does not need to evaluate compatibility under Article 8A(2). The list of circumstances are:

- when a data subject has given fresh consent for the new purpose (Article 8A(3)(a));
- when the processing is for research (historical and scientific), archiving in the public interest and statistical purposes (Article 8A(3)(b)) and is carried out in accordance with Article 84B UK GDPR;
- when the processing of personal data is carried out for the purposes of ensuring that it complies with Article 5(1) of the UK GDPR, or demonstrating that it does (Article 8A(3)(c)). For example if a controller is seeking to pseudonymise personal data (and this was not anticipated or notified at the point of data collection), then this is permitted through Article

8A(3)(c). In most cases pseudonymisation or other data security measures will be considered compatible further processing or will have been signalled at the point of collection. However, where the original lawful basis for the collection of personal data was consent, the compatibility route would not be available.

- when the controller's purpose is among the purposes outlined in Annex 2 (Article 8A(3)(d));
- where the processing is necessary to safeguard an interest in Articles 23(1)(c) to (j) (for example, important objectives of public interest, in particular an important economic or financial interest of the UK, including monetary, budgetary and taxation matters, public health and social security (A23(1)(e)) and is authorised by legislation or a rule of law (Article 8A(3)(e)).

146. New Article 8A(4) outlines the additional restrictions placed on further processing of personal data that was originally collected on the basis of consent (through Article 6(1)(a) UK GDPR). Further processing of such data is

only permitted in four circumstances: (i) if fresh consent is sought and obtained under Article 8A(3)(a); (ii) if the processing is carried out for the purposes of ensuring that processing of personal data complies with Article 5(1) of the UK GDPR, or demonstrating that it does, (iii) if the processing meets a condition in Annex 2 (see Article 8A(3)(d)), or (iv) if it is necessary to meet a safeguard in Articles 23(1)(c) to (j) and is authorised by an enactment or a rule of law (see Article 8A(3)(e)). In cases (iii) and (iv), the controller must additionally consider whether it is reasonable to seek the data subject's consent. Further processing of personal data that was originally collected in reliance on the lawful ground of consent (Article 6(1)(a) UK GDPR) is not permitted on the basis of a compatibility assessment (Article 8A(2)) or when processing is for historical, scientific, or statistical purposes, or for archiving in the public interest (Article 8A(3)(b)).

147. The Secretary of State has the power under new Article 8A(5) to amend the list of conditions in Annex 2 that are to be treated as compatible with the original purpose. The power enables the Secretary to add to or vary

the conditions or omit conditions added by regulations. Any conditions added to the Annex by primary legislation cannot be removed through use of this power. Pursuant to Article 8A(6), a new condition can only be added to Annex 2 where it meets one of the important public interest objectives outlined in Article 23(1)(c)-(j) UK GDPR. Article 8A(7) provides that the power can make provision to specify processing such as reference to the controller or the provision of Article 6(1) relied on for the purposes of processing. The power is subject to the affirmative procedure by virtue of new Article 8A(8).

148. Subsection(6) of clause 6 introduces Schedule 2.

149. Subsections(7)-(9) make amendments equivalent to those made to Article 5(1)(b) UK GDPR by clause 6 (2) to sections 36(1) and 87(1) of the Data Protection Act 2018. These sections set out the purpose limitation rules for law enforcement processing (s.36(1)) and for Intelligence Services processing (section 87(1)). The amendments clarify that the rules around further processing apply to personal data collected from a data subject or otherwise

by the controller or a processor currently processing that data.

150. Subsection (10) removes the purpose limitation limb of paragraph 5(1)(b) from the definition of "the listed GDPR provisions" in Part 1 of Schedule 2 to the Data Protection Act 2018 as the exemptions from the purpose limitation in that Part have now been added to new Annex 2 to the UK GDPR by virtue of Schedule 2.

Special categories of personal data

Clause 7: Elected representatives responding to requests

151. Clause 7 makes amendments to paragraph 23 of Schedule 1 to the Data Protection Act 2018, which permits elected representatives to process special category data in connection with the discharge of their functions and following a request made by an individual for them to act on their behalf. Under the previous legislation, an elected representative in the House of Commons, National Assembly for Wales, Scottish Parliament or Northern Ireland Assembly could only rely on this provision for four days after

leaving office after a general election. Clause 7 extends that period of time from four to thirty days.

Data subjects' rights

Clause 8: Vexatious or excessive requests by data subjects

152. Clause 8 amends Article 12 of the UK GDPR. Clause 8 (3) inserts into the UK GDPR new Article 12A. New Article 12A permits a controller to charge a reasonable fee for or refuse to act on a request which is 'vexatious or excessive'. This replaces the previous provision in Article 12 to refuse or charge a reasonable fee for 'manifestly unfounded or excessive' requests.

153. Subsection (3) new Article 12A(1) applies to all requests under Articles 15 to 22 and 34 of the UK GDPR.

154. Subsection (3) new Article 12A(2) enables data controllers to charge a reasonable fee for or refuse to act on requests which are considered 'vexatious or excessive'. The provision captures a clearer set of requests which a controller can charge a reasonable fee for or refuse to act on. Where a controller

charges for a request under new Article 12A(2)(a), section 12 of the DPA 2018 allows the Secretary of State, through secondary legislation, to place limits on these fees.

155. Subsection (3) new Article 12A(3) clarifies that it is the responsibility of the controller to prove that a request is vexatious or excessive, particularly when this is questioned by the data subject or the Commissioner.

156. Subsection (3) new Article 12A(4) provides more detail on which factors controllers should take into account when assessing if a request is ‘vexatious or excessive’. The list of factors is non-exhaustive and a request does not have to satisfy all factors for the provision to apply. These factors may be considered, where relevant, with regard to the request itself, the data subject the request relates to, and any third party which has submitted the request on behalf of a data subject. A request should also be considered taking account of other relevant circumstances and within the context it is made.

157. Subsection (3) new Article 12A(5) provides examples of requests which could be considered ‘vexatious’. This is a non-

exhaustive list and does not capture all types of vexatious requests. The examples given are common situations where a request from a data subject (or a third party submitting a request on a data subject's behalf) might be considered vexatious, also taking into account the factors for consideration in 12A(4), where relevant.

158. Subsection (6) changes section 53 of Part 3 of the DPA 2018 to permit law enforcement controllers to charge a reasonable fee or refuse a request where it is 'vexatious or excessive', aligning with changes made in the UK GDPR by clause 8 (3). This provision applies to all requests under sections 45, 46, 47 or 50 of the DPA 2018. This includes subject access requests made under section 45 and other requests such as requests for erasure under section 47.

159. Subsection (6) retains the ability for controllers to refuse or charge a reasonable fee for a request which is deemed 'vexatious' or 'excessive'. Section 53(4) of the DPA 2018 allows the Secretary of State, through secondary legislation, to place limits on these fees. It is the responsibility of the controller to prove that a request is vexatious or excessive,

particularly when this is questioned by the data subject or the Commissioner.

160. Subsection (8) changes Part 4 of the DPA 2018 to introduce the possibility for controllers to refuse a request under section 94 (which regulates rights of access to information by the data subject under Part 4) where the request is deemed ‘vexatious’ or ‘excessive’. It is the responsibility of the controller to prove that a request is vexatious or excessive, particularly when this is questioned by the data subject or the Commissioner.

161. Subsection (10) adds new section 204A to the DPA 2018. This section provides more detail on which factors controllers should consider when assessing if a request is ‘vexatious or excessive’ for the purposes of the DPA 2018.

Clause 9: Time limits for responding to requests by data subjects

162. Clause 9 changes the time limits for responding to requests from data subjects. Clause 9 (3) makes provisions to amend references to time periods across the

legislation on the right of access to refer to the 'applicable time period'. It sets out what the applicable time period is in different circumstances.

163. In general, requests from data subjects must be responded to within one month of being received. Clause 9 (3) new Article 12B(1) and (2) clarify the circumstances where this response time is different and what the time period is instead.

164. Subsection (3) new Article 12B (3) retains the provision enabling a controller to extend the standard one month response period by a further two months if the request is complex. For example, this two-month extension may be necessary due to the number of requests submitted in relation to the data subject. New Article 12B (4) explains that a controller must inform the data subject of the extended response time and the reason for the delay within one month of receiving the request.

165. Subsection (3) new Article 12B (5) allows the response time to a subject access request submitted under Article 15 to be paused to seek clarification on the information requested by the data subject. This only applies where

the controller cannot reasonably proceed with responding to the subject access request without this information. Once the necessary clarification is received, the response time resumes. This provision was previously set out in the Commissioner's guidance.

166. Subsection (5) amends section 45 of Part 3 of the Data Protection Act 2018, section 45 sets out the right of access afforded to data subjects under Part 3 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, as the rights to rectification, erasure or restriction on processing. This clause clarifies that controllers must respond to subject access requests before the end of an applicable time period as added to section 54 of the DPA 2018 under clause 9 (6).

167. Subsection (6) amends section 54 to make supplementary provisions about the extension of the applicable time period for responding to subject access requests to provide information to the data subject in accordance with section

48 DPA 2018. Clause 9 (6) subsection (3A) replicates the provision in clause 9 (3) new Article 12B (3) to allow the law enforcement controllers to also extend the applicable time period by two further months where it is necessary to do so for reasons of complexity of the request or on account of the number of requests. The controller is required to give notice to the data subject about the extension under subsection (3B).

168. Subsection (6) subsections (3C) and (3D) make amendments to the time requirements controllers are subject to when responding to a subject access request in Part 3 DPA 2018. These subsections replicate the new provision in clause 9 (3) new Article 12B (5) for a controller to be able to pause the response time if further information is required in order to proceed.

169. Subsection (7) makes amendments to section 94 of the DPA 2018; section 94 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. This subsection makes similar amendments as clause 9 (6) to allow Part 4

controllers to extend the applicable time period by two further months where it is necessary to do so for reasons of complexity or on account of the number of requests. The controller is required to give notice to the data subject about the extension before the end of one month.

Clause 10: Information to be provided to data subjects

170. Clause 10 amends Article 13 and Article 14 of the UK GDPR. These two articles specify the information that should be provided to data subjects at the point of data collection, either when collected directly from the data subject (Article 13) or obtained indirectly (Article 14).

171. Article 13(3) of the UK GDPR currently provides that when a data controller intends to further process personal data (which is the reuse of personal data for a separate purpose than that for which it was originally collected), they are required to provide additional information to the data subject. The content of these information requirements is laid out in Article 13(2). Clause 10(1) adds an additional paragraph to the end of Article 13 which creates an exemption from Article 13(3) for

processing for research, archiving and statistical (RAS) purposes where there would be a disproportionate effort to provide the required information to data subjects and where the research is in line with the safeguards for research found in Article 84B of the new Chapter 8A of the UK GDPR by virtue of clause 24.

172. New paragraph 6 inserted by clause 10 (1) provides a non-exhaustive list of factors for the controller to determine what could constitute a disproportionate effort for the purposes of the new exemption.

173. Clause 10 (2) also amends Article 14 of the UK GDPR. Clause 10 (2)(a)(i),(iii) and (iv) all make minor and technical changes to parts of paragraph 5 of Article 14. These changes do not alter the meaning or current application of the Article 14 but are made to accommodate other changes to Article 14 made by clause 10.

174. Currently, Article 14(5)(b) of the UK GDPR creates a disproportionate effort or impossibility exemption for all processing where the data was not collected directly from data subjects. It also sets out RAS purposes as an example in a non-exhaustive list of when

the exemption may be used. Article 14(5)(b) is being removed and replaced by clause 10 (2), which splits the current disproportionate effort exemption into two new subsections and removes the example of RAS purposes from the non-exhaustive list. This does not materially affect how the current exemption in Article 14 operates, but does make it clearer that the exemption applies to all processing activities.

175. Clause 10 (2)(b) inserts two new paragraphs at the end of Article 14. Paragraph 6 replicates the non-exhaustive list of examples of disproportionate effort being inserted into Article 13 by virtue of section (1) of this clause.

176. Paragraph 7 adds the same safeguard for the disproportionate effort or impossibility exemption as currently found in Article 14(5)(b) which is being removed by virtue of clause 10 (2)(a)(ii).

Clause 11: Data subject's rights to information: legal professional privilege exemption

177. Clause 11 inserts a new section 45A into the DPA 2018 which explicitly introduces an exemption for material which is subject to legal professional privilege or, in Scotland, to confidentiality of communications. Legal Professional Privilege protects all communications between a professional legal advisor and their clients.

178. Section 45A(3) disapplies the requirement that competent authorities inform the data subject that they are relying on a claim to legal professional privilege (or duty of confidentiality in Scotland) and their reason for doing so where this would undermine the claim (or duty) thereby allowing them to provide a 'neither confirm nor deny' response.

Automated decision-making

Clause 12: Automated decision-making

179. Article 22 of the UK GDPR sets out the conditions under which solely automated decisions, including profiling, that produce legal or similarly significant effects on data subjects may be carried out. It restricts such

activity to three conditions: (i) where necessary for entering into, or the performance of, a contract between a controller and a data subject; (ii) where such activity is required or authorised by law; or (iii) where a data subject has provided explicit consent.

180. Clause 12 replaces Article 22 of the UK GDPR with new Articles 22A-D whereby automated decision-making of this nature is not restricted to those three circumstances.

181. Article 22A(1)(a) defines a decision based on solely automated processing as one that involves no meaningful human involvement. Article 22A(1)(b)(i) and (ii) set out the meaning of a significant decision as one that produces legal or similarly significant effects on a data subject.

182. Article 22A(2) requires controllers to consider, among other things, the extent to which a decision has been taken on the basis of profiling when establishing whether or not human involvement has been meaningful.

183. Article 22B(1)-(3) prohibits the use of special categories of data for such activities unless one of two conditions is met.

The first condition is that a data subject has provided explicit consent to being subject to such processing.

The second condition, as an alternative, entails the joint fulfilment of two requirements:

(i) The first requirement is that such activity is necessary for:

- entering into, or the performance of, a contract between a data subject and controller, Article 6(1)(b) UK GDPR; or
- that it is required or authorised by law, which includes the reasonable use of such processing to comply with legal obligations, Article 6(1)(c) UK GDPR or where processing is necessary for the performance of a public task carried out in the public interest or in the exercise of official authority (for example, a public body's tasks, functions, duties or powers), Article 6(1)(e) UK GDPR.

(ii) The second requirement is that the activity also satisfies Article 9(2)(g); that is, the activity must be in the substantial public interest.

184. Article 22B(4) prohibits reliance on new Article 6(1)(ea) when taking significant decisions based solely on automated processing. This means that where such a decision is taken for the purposes of detecting, investigating, or preventing crime or apprehending offenders, or any other activity in Annex 1 to Schedule 1, a different lawful ground in Article 6(1) will need to be identified. This could include the legitimate interests lawful ground under Article 6(1)(f), providing that the requirements associated with that ground can be satisfied.

185. Article 22C(1) and C(2) set out the safeguards for automated decision-making in scope and replace the provisions at Article 22(3) and Article 22(3A) of the UK GDPR and section 14 of the DPA 2018. The clause places a requirement on controllers to provide information to the data subject relating to significant decisions being taken through solely automated processing. Where appropriate, this may include notifying data subjects after such a decision has been taken or informing them of the logic involved in producing that particular decision. They also set out the rights of a data subject to express their point of view with

respect to such decisions, to contest them, and to seek human intervention. This means controllers must put in place suitable measures enabling data subjects to do this. These safeguards would enable data subjects to challenge solely automated decisions that produce significant effects on them, regardless of the legal basis on which they are taken. It would also ensure that under such circumstances, controllers will be required to review the decisions in question, and take suitable measures to correct them if they have produced a wrongful outcome.

186. Article 22D(1) and D(2), confers regulation making powers to the Secretary of State to provide directly, and/or, through secondary legislation for the purposes of:

(i) Article 22A(1)(a) cases that are, or are not, to be taken to have meaningful human involvement and

(ii), Article 22A(1)(b)(ii) describe what is, or is not, to be taken as a significant decision.

The powers in Article 22D(3) enables the Secretary of State to bring in regulations made under new Article 22D(1) and new Article 22D(2) to amend Article 22A directly. These

provisions will ensure that additional legal clarity on the circumstances in which safeguards must apply can be introduced if and when necessary and appropriate. For example, this might be necessary in light of the rapid advancement and adoption of technologies related to automated decision-making that may inform when meaningful involvement can be said to have taken place, as well as changing societal expectations of what constitutes a significant decision in a privacy context.

187. Article 22D(4) confers a regulation making power to the Secretary of State to add and amend safeguards set out in Article 22C directly. Article 22D(5) supplements this power allowing for any regulations made under Article 22D(4) to (i) add or vary existing and future safeguards listed in Article 22C and (ii) permits the removal of any new safeguards provided.

188. Clause 12(3) amends equivalent provisions on automated decision making in Part 3 of the DPA, repealing sections 49 and 50 and replacing them with sections 50A, 50B, 50C & 50D. These new sections take a consistent approach with new Articles 22A – D of the UK GDPR.

189. Section 50A defines ‘a decision based on solely automated processing’, as one that involves no meaningful human involvement in the taking of the decision. Section 50A(1)(b)(i) and (ii) defines a significant decision as one that produces an adverse legal or similarly adverse significant effect on a data subject. Section 50 restricts the definition of significant effects to only those that would have an adverse impact on the data subject. This is because under Part 3, it tends to be more clear-cut whether a decision will have an adverse significant effect on the data subject, whereas the effect of a significant decision under UK GDPR may be more nuanced.

190. Section 50A(2) mirrors the requirement for controllers to consider, among other things, the extent to which a decision has been taken on the basis of profiling when establishing whether or not human involvement has been meaningful.

191. Section 50B restricts the processing of sensitive personal data (the equivalent of special categories of data under the UK GDPR) via automated processing to situations where either the data subject has given their consent or the processing is authorised by law.

Unlike Article 22B(3)(a), processing for the purposes of entering into a contract between the data subject and the competent authority is not a valid condition for processing such data. This is because it is not considered likely that such a situation would ever arise under Part 3.

192. Section 50C(1) mirrors the list of safeguards available to data subjects. Section 50C(3) provides an exemption to the requirement to apply the safeguards provided that:

- it is necessary for one of the reasons set out under section 50C(4), such as to prevent the obstruction of an inquiry or, to protect national security;
- it is carried out as soon as is reasonably practicable (in most cases, the human review should take place immediately); and
- the reconsideration of the decision involves some level of meaningful human involvement.

193. Section 50D mirrors the powers of the Secretary of State to make further provisions

about automated decision-making set out under Article 22D.

194. Clause 12(4) and (5) makes amendments to sections 96 and 97 of the DPA 2018. The amendment to section 96 provides a definition of automated decision making for Part 4 of the DPA 2018. A decision is based on entirely automated processing if the decision-making process does not include an opportunity for a human being to accept, reject or influence the decision. Minor consequential changes have been made to section 97 to reflect this new definition.

Obligations of controllers and processors

Clause 13: General obligations

195. Clause 13 (1) intended to clarify the terminology in Article 24(1) by replacing the requirement to implement “appropriate technical and organisational measures” with “appropriate measures, including technical and organisational measures”. Similar clarification is made to Article 25(1) and Article 28(1), (3) and (4)(e) by clause 12 (2) and (3). These changes will give data controllers more

flexibility in terms of the measures they put in place to demonstrate and manage risk.

196. Corresponding amendments are made to sections 55, 56, 57, 59 and 103 in Part 3 of the DPA 2018 by sub-clauses (5) to (10).

197. Schedule 9 makes a minor and technical amendment to improve the terminology in Articles 24(3), Article 25(3) and Article 32(1).

Clause 14: Removal of requirement for representatives for controllers etc outside the UK

198. Clause 14 seeks to omit Article 27 from UK GDPR in its entirety. As a result of omitting Article 27, controllers and processors who must comply with the UK GDPR pursuant to Article 3(2) UK GDPR will no longer be required to appoint a UK based representative.

199. The function of the representative is to facilitate liaison and effective communication between such controllers and processors and UK stakeholders (such as UK data subjects and the ICO). Given that legal requirements for such communication already exist elsewhere in UK GDPR, the removal of Article 27 will allow organisations to decide for themselves the best way to comply with the requirements

for effective communication under the legislation, which may still include the appointment of a UK based representative.

200. The clause then makes a number of amendments to the UK GDPR and DPA 2018 as a consequence of the removal of Article 27.

Clause 15: Senior responsible individual

201. Clause 15 replaces the requirements on Data Protection Officers in Articles 37 to 39 of the UK GDPR and sections 69 to 71 of the DPA 2018. It introduces new requirements for controllers and processors to designate a "senior responsible individual" to be responsible for data protection risks within their organisations or delegate that task to suitably skilled individuals.

202. Clause 15 (2) adds new Article 27A to the UK GDPR. New Article 27A(1) sets out the criteria for when a senior responsible individual needs to be appointed, namely where the controller or processor is a public body (except for courts or tribunals acting in their judicial capacity) or where they are carrying out processing that is likely to result in a high risk to individuals. This could include, for example, where the organisation is processing special

category data on a large scale or data relating to criminal convictions, or using innovative technologies to process large volumes of personal data. Organisations would not need to appoint a senior responsible individual if their processing activities were low risk.

203. New Article 27A (2) provides that controllers or processors who are subject to these requirements must appoint one senior responsible individual to take responsibility for the list of tasks in Article 27C.

204. New Article 27A (3)(a) requires the senior responsible individual to be part of the organisation's senior management. New Article 27A(3)(b) makes it clear that the position of the senior responsible individual can be carried out jointly by more than one person on a job-share basis.

205. New Article 27A (4) requires controllers or processors to make the contact details of the senior responsible individual publicly available and ensure those details are sent to the Commissioner.

206. New Article 27A (5) defines the meaning of 'senior management' for the purposes of these provisions.

207. New Article 27B requires the senior responsible individual to be responsible for the tasks set out in Article 27B (2) if they are a data controller; or the tasks in Article 27C(4) if they are a data processor.

208. New Article 27B (5) requires the senior responsible individual to delegate his or her tasks to another person if performing them would result in a conflict of interest with his or her own role.

209. New Article 27B (6)(a)-(c) lists the factors which the senior responsible individual must consider should they decide to delegate tasks to another person.

210. New Article 27C sets out the position of the senior responsible individual. Article 27B (1) requires the data controller or processor to ensure that the senior responsible individual is appropriately resourced. Article 27C(2) makes it clear that the senior responsible individual must not be dismissed or penalised for performing its tasks under Article 27C.

211. New Article 27C (3) and (4) states that the delegated individual must not be instructed about the performance of its tasks unless it is given by the senior responsible individual.

212. Clause 15 (3) repeals the current requirements in Articles 37 to 39 of the UK GDPR on Data Protection Officers.

213. Clause 15 (4) introduces similar changes to those outlined above in respect of senior responsible individuals to Part 3 of the Data Protection Act 2018.

214. Clause 15 (5) adds new section 58A which introduces a duty for controllers and processors carrying out certain processing activities under Part 3 of the DPA 2018 to designate a senior responsible individual.

215. New section 58A(3)(a) requires the senior responsible individual to be part of the organisation's senior management. New section 58A(3)(b) makes it clear that the position of the senior responsible individual can be carried out jointly by more than one person on a job-share basis.

216. New section 58A(4) requires controllers or processors to make the contact details of the senior responsible individual publicly available and ensure those details are sent to the Commissioner.

217. New section 58A(5) defines the meaning of ‘senior management’ for the purposes of these provisions.

218. New section 58B requires the senior responsible individual to be responsible for the tasks set out in section 58B(2) if they are a data controller; or the tasks in section 58C(4) if they are a data processor.

219. New section 58B(5) requires the senior responsible individual to delegate his or her tasks to another person if performing them would result in a conflict of interest with his or her own role.

220. New section 58B (6)(a)-(c) lists the factors which the senior responsible individual must consider should they decide to delegate tasks to another person.

221. New section 58C sets out the position of the senior responsible individual. Section 58C(1) requires the data controller or processor to ensure that the senior responsible individual is appropriately resourced. Article 58C(2) makes it clear that the senior responsible individual must not be dismissed or penalised for performing its tasks under section 58C.

222. New section 58C (3) and (4) states that the delegated individual must not be instructed about the performance of its tasks unless it is given by the senior responsible individual.

Clause 16: Duty to keep records

223. Clause 16 removes Article 30 of the UK GDPR and section 61 of the DPA 2018 on records of processing activities and replaces them with new requirements on record-keeping.

224. Clause 16 (4) inserts new Article 30A into the UK GDPR which requires the controller or processor to maintain an appropriate record about the personal data.

225. New Article 30A (1) provides that a controller or processor is exempt from the duty to keep records, unless they are carrying out high risk processing activities.

226. New Article 30A (3) set out the information which must be included in the record of the data controller. New Article 30A(6) sets out the requirements for the data processor's record.

227. New Article 30A (9) sets out the factors which controllers and processors must consider when deciding what is an

‘appropriate’ record. They include factors such as the nature, scope and context of the processing; the risks their processing poses to individuals; and the resources available to the controller or processor.

228. New Article 30A (4) and (7) provide that where possible the record must include information as to how the controller or processor will ensure that the data is secure.

229. Clause 16 (6)and (8) removes section 61 (records of processing activities) from the DPA 2018 and subsection 42(4) which required additional information to be kept in records maintained under section 61 in certain circumstances related to sensitive processing. Clause 16 (9) inserts a requirement for the controller or processor to maintain appropriate records of personal data.

230. New section 61A (2) set out the information which must be included in the record of the data controller. New section 61A (5) sets out the requirements for the data processor’s record.

231. New section 61A (8) sets out the factors which controllers and processors must consider when deciding what is an

'appropriate' record. They include factors such as the nature, scope and context of the processing; the risks their processing poses to individuals; and the resources available to the controller or processor.

232. New section 61A (3) and (6) provide that where possible the record must include information as to how the controller or processor will ensure that the data is secure.

Clause 17: Logging of law enforcement processing

233. The DPA 2018 introduced a requirement in section 62 that competent authorities keep logs of their processing activities including the collection, alteration, consultation, disclosure, combination, and erasure of personal data.

234. The purposes for which these logs may be used are set out in subsection (4). One of these purposes is self-monitoring. This is in order to assist competent authorities with disciplinary proceedings such as improper access or unauthorised disclosure. For example, if an officer or member of police staff was suspected of inappropriately accessing the Police National Computer to check on neighbours, family or friends, the log should

show details of when the record was accessed and, where possible, by whom.

235. Clause 17 only removes the requirement for a competent authority to record a 'justification' in the logs when consulting or disclosing personal data. This is because in an investigation concerning inappropriate use, it is unlikely the justification given by the individual under investigation for accessing the personal data would be sufficiently reliable for use in the decision-making process. It is also technologically challenging for systems to automatically record the justification without manual input. The remaining requirements in section 62 DPA 2018, relating to the logs of consultation and disclosure, will remain, such as the need to record the time and date and, as far as possible, the identity of the person accessing the log.

Clause 18: Assessment of high risk processing

236. Clause 18 amends Article 35 of the UK GDPR and section 64 of the DPA 2018.

237. Clause 18 (2) amends the heading of Article 35 of the UK GDPR from "Data Protection Impact Assessments" to 'Assessments of high risk processing' .

238. Clause 18 (3) omits or amends a number of requirements in the current Article 35. Under the amended provisions in Article 35(7), the data controller's assessment of high risk processing will need to include a summary of the purposes of the processing; an assessment of whether the processing is necessary and the risks it poses to individuals; and a description of how the controller intends to mitigate any risks.

239. Clause 18(3) also omits Articles 35(4) and 35(5). It replaces these provisions with a new duty under Article 57(1)(k) for the ICO to produce and publish a document containing examples of types of processing which the Commissioner considers are likely to result in a high risk to the rights and freedoms of individuals for the purposes of all three new compliance obligations in Articles 27A, 30A and 35.

240. Clause 18 (7) omits or amends the heading of section 64 of the DPA 2018 from 'data protection impact assessments' to 'assessment of high risk processing'.

241. Clause 18 (7) also amends section 64 (3). Under the amended provisions in section

64(3), the data controller's assessment of high risk processing will need to include a summary of the purposes of the processing; an assessment of whether the processing is necessary and the risks it poses to individuals; and a description of how the controller intends to mitigate any risks.

Clause 19: Consulting the Commissioner prior to processing

242. Clause 19 (1) amends Article 36 of UK GDPR (prior consultation) in accordance with subsection (2) and (3). Clause 19 (2) makes optional the previous requirement for controllers to consult the Commissioner prior to processing where an assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

243. Schedule 4 section 22 repeals paragraph 26(9)(c)(ii) of Schedule 2 to the DPA 2018 (exemption from Article 36 UK GDPR for journalistic, academic, artistic and literary purposes) in consequence of the changes

made to that Article by clause 19(2). Given that Article 36(1) UK GDPR (prior consultation) is amended to the effect that the previous requirement for controllers to consult the Commissioner becomes a power to do so, the exemption is no longer required as there is no longer a duty to be exempt from.

244. Schedule 4 section 10 subsection (2) amends Article 83 of UK GDPR (general conditions for imposing an administrative fine) by inserting “including any consultation under Article 36(1)”. It allows the Commissioner to consider any relevant prior consultation under Article 36 when imposing administrative fines on a data controller.

245. Clause 19 (4) amends section 65(2) and (3) of the Data Protection Act 2018, which relates to the requirement to notify the Commissioner (prior consultation), in accordance with Clause 19 (5) and (6). Clause 19 (5) makes optional the previous requirement to inform the Commissioner prior to processing where a risk assessment under section 64 indicates that there is a high risk to the rights and freedoms of the individuals (in the absence of measures to mitigate the risk).

Clause 20: General processing and codes of conduct

246. Clause 20 amends Article 41 of the UK GDPR to clarify that accredited monitoring bodies are only required to notify the Information Commissioner if they suspend or exclude a person from a code under the UK GDPR. This reflects the Commissioner's operational approach and ensures consistency with new Regulation 32B of the Privacy and Electronic Communications Regulations 2003 which is inserted by clause 91.

Clause 21: Law enforcement processing and codes of conduct

247. Clause 21 inserts a new section 71A into the DPA 2018 which enables expert public bodies, who have sufficient knowledge and experience, to create codes of conduct. These are voluntary, sector-specific pieces of guidance which enable controllers to identify and resolve key data protection challenges in their sector and demonstrate compliance with the data protection legislation. Subsection (4) sets out a non-exhaustive list of the areas that may be covered when drawing up a code of conduct; this includes, for example, guidance

on the information that controllers must provide to the public and to data subjects. Expert public bodies are encouraged to consult with relevant stakeholders when drawing up, amending or extending a code of conduct to ensure that it appropriately reflects the processing activities set out under Part 3 of the DPA 2018.

Clause 22: Obligations of controllers and processors: consequential amendments

248. Clause 22 contains amendments consequential on this group of sections.

International transfers of personal data

Clause 23: Transfers of personal data to third countries and international organisations

249. Clause 23 inserts Schedules 5, 6, and 7, which amend Chapter 5 of the UK GDPR and Chapter 5 of Part 3 of the DPA 2018 to reform the UK's regime for international transfers of personal data.

Safeguards for processing for research etc purposes

Clause 24: Safeguards for processing for research etc purposes

250. Clause 24 amends the UK GDPR by creating a new Chapter 8A and makes related consequential amendments. This new chapter consists of four new articles which combine the existing safeguards currently found in Article 89 of the UK GDPR and section 19 of the DPA 2018 for data processing for archiving in the public interest, scientific, historic and statistical research purposes. Clause 24 (2) amends the UK GDPR by creating a new article, 84A. Article 84A outlines the categories of data processing that fall within the scope of this chapter (processing for scientific or historical research, archiving in the public interest and statistical purposes) and creates a new acronym, 'RAS purposes' to refer to these purposes.

251. Clause 24 (2) also amends the UK GDPR by creating two new articles, 84B and 84C. These new articles set out the safeguards required when processing personal data for RAS purposes. This includes that the

processing must not cause substantial damage or substantial distress to a data subject and it must also include technical and organisational measures for the purpose of ensuring respect for the principle of data minimisation. In addition, the processing must not be carried out for the purposes of measures or decisions with respect to a particular data subject, unless it is for approved medical research. Clause 24 (2) also replicates the definition of “approved medical research" from section 19 of the DPA 2018.

Clause 25: Section 22: consequential provision

252. Clause 25 makes consequential amendments to the UK GDPR, the DPA 2018 and the Mental Health (Care and Treatment) (Scotland) Act 2003. These amendments are required as a result of the changes made in clause 25 which move provisions on the safeguards for RAS purposes for section 19 of the DPA 2018 to the new chapter 8A of the UK GDPR.

National security

Clause 26: National Security Exemption

253. Clause 26 inserts a new section 78A into Part 3 of the DPA 2018, providing an exemption from specified provisions in Part 3 when required for the purposes of safeguarding national security. The provisions that may be disapplied in such circumstances are listed in subsection (2) and include most of the data protection principles, the rights of data subjects, certain obligations on competent authorities and processors, and various enforcement provisions. Part 3 of the DPA 2018 already enables competent authorities to apply restrictions to specified rights where necessary to protect national security, but this new exemption ensures that there is consistency in approach by competent authorities by mirroring the national security exemptions already available to competent authorities under the UK GDPR (section 26 of the DPA 2018) and Part 4 (section 110 of the DPA 2018).

Intelligence Services

Clause 27: Joint processing by intelligence services and competent authorities

254. Clause 27 amends Part 4 of the DPA 2018 to enable joint processing between a qualifying competent authority (or authorities) and an intelligence service (or intelligence services), under Part 4 of the DPA 2018. This enables the controllers to process the data within a single, common regime. The controls and safeguards under Part 4 will apply to all such joint processing.

255. Subsection 2 of Clause 27 amends section 82 of the DPA 2018, changing the scope of Part 4. Currently Part 4 only applies to processing by or on behalf of the Intelligence Services. This amendment makes clear that Part 4 also applies to the processing of personal data by a qualifying competent authority where the processing is the subject of a designation notice.. New subsection (2A) provides a power to the Secretary of State to make regulations to specify competent authorities (as defined in Part 3 of the DPA) who can be regarded as “qualifying competent authorities”, so able to apply for or be issued

with a designation notice. New subsection (4) provides that any such regulations are subject to the affirmative procedure.

256. Subsection 3 of clause 27 inserts new sections, 82A – 82E, that impose the conditions for designation notices.

257. 82A enables qualifying competent authorities (as specified in Regulations) to jointly apply for a notice from the Secretary of State permitting them to have a joint controller relationship under Part 4 of the DPA 2018. The Secretary of State must be satisfied that the intended processing is required for the purposes of safeguarding national security. Before giving a designation notice, the Secretary of State must consult with the Commissioner, and they may also consult with other relevant public or regulatory bodies as appropriate.

258. 82B provides for rules governing the duration of a designation notice. Notices cease to be in force after a period of 5 years or a shorter period if specified in the notice issued by the Secretary of State.

259. 82C imposes conditions on the review and withdrawal of a designation notice. It requires a

designation notice to be reviewed at least annually by the Secretary of State.

260. A designation notice may be withdrawn by the Secretary of State at any time, following a review and when some or all of the processing to which the notice applies is no longer required for the purposes of safeguarding national security.

261. When considering when a withdrawal notice should come into force, the Secretary of State must take into account the time needed for controllers to effect an orderly transition to new arrangements for the processing of that data. During the transition period and prior to the withdrawal notice coming into effect, the processing of data falling within the terms of the notice by a joint controller would continue to be subject to Part 4 DPA 2018. For example, joint processing activities such as transiting data in readiness for the notice being withdrawn would continue to be subject to Part 4 DPA 2018. When a notice is not in force or when processing is outside the scope of a notice, Part 3 of the DPA 2018 or the UK GDPR will apply to any processing by the competent authority, depending on its purpose.

262. 82D requires the Secretary of State to provide a copy of the designation notice to the Commissioner and the Commissioner must make available to the public a record of that designation notice whilst it is in force, with the assumption of transparency.

263. 82E allows a designation notice to be appealed to the tribunal if a person is directly affected by the notice.

Clause 28: Joint processing: consequential amendments

264. Subsections 2 – 8 of clause 26 makes necessary consequential amendments to the DPA 2018 to reflect the changes made by clause 25, which will enable joint processing between a qualifying competent authority (or authorities) and an intelligence service (or intelligence services), under Part 4 of the DPA 2018.

Information Commissioner's role

Clause 29: Duties of the Commissioner in carrying out functions

265. Clause 29 amends Part 5 of the DPA 2018 by inserting new sections providing for a

principal objective and general duties for the Commissioner when carrying out functions under the data protection legislation. It also makes provision for the Commissioner to prepare and publish a strategy and introduces new reporting requirements.

266. Subsection (2) of clause 29 omits section 2(2) (duty of Commissioner when carrying out functions) of the DPA 2018. This now forms part of the new principal objective at new section 120A of the DPA 2018.

267. New section 120A introduces a new principal objective for the Commissioner. To meet this objective when carrying out functions under the data protection legislation, the Commissioner should aim to secure an appropriate level of protection for personal data, having regard to the interests of data subjects, controllers and others and matters of general public interest; and to promote public trust and confidence in the processing of personal data.

268. New section 120B sets out new duties for the Commissioner when carrying out data protection functions. This includes duties to have regard to the desirability of promoting

innovation and competition. There is also a new duty to have regard to the importance of preventing, investigating and detecting criminal offences and a new duty to have regard to the need to safeguard public and national security.

269. New section 120C requires the Commissioner to prepare and publish a forward looking strategy. This should detail how the Commissioner will discharge functions under the data protection legislation in relation to duties under new sections 120A and 120B. It should also detail how the Commissioner will discharge data protection functions in relation to duties under section 108 of the Deregulation Act 2015 which requires the Commissioner to have regard to the desirability of promoting economic growth when exercising a regulatory function. In addition, there is a requirement for the strategy to set out how data protection functions will be carried out in accordance with the duty under section 21 of the Legislative and Regulatory Reform Act 2006 to have regard to the principles that regulatory activities should be carried out in a way which is transparent, accountable, proportionate and consistent and should be targeted only at cases in which action is needed.

270. New section 120C does not require the strategy to take a particular form and it is envisaged that this obligation can be met by a standalone report. The Commissioner must review and revise the strategy as needed as outlined in 120C(2) and must publish the strategy and any revised strategy, as outlined in 120C(3).

271. New section 120D outlines the duty for the Commissioner to consult, when giving consideration to how the manner in which the Commissioner exercises functions under the data protection legislation may affect economic growth, innovation and competition. An example of such instances could be issues relating to emerging technology. This consultation should be conducted at such times as the Commissioner considers appropriate.

272. New section 120D(2) defines the scope of this consultation requirement, outlining that it requires the Commissioner to consult other regulators and other such persons as the Commissioner considers appropriate in relation to economic growth, innovation and competition.

273. Clause 29 subsection (4) inserts a new requirement for the Commissioner to report on what has been done to comply with the duties during a reporting period. This will also include a review of the strategy published under new section 120C and a summary of what the Commissioner has done to comply with the consultation duty under new 120D. This reporting requirement will be an additional part of the Commissioner's annual reporting requirements to Parliament under the DPA 2018.

274. Clause 29 subsection (5) inserts the requirement for the Commissioner to prepare the first strategy as set out in 120C within 18 months of this requirement coming into force.

Clause 30: Strategic priorities

275. Clause 30 amends Part 5 of the DPA 2018 by inserting new sections that make provisions for the introduction of a Statement of Strategic Priorities ('the Statement'). The Statement will set out the government's data protection priorities to which the Commissioner must have regard when carrying out their data protection functions.

276. New section 120E outlines the process for

designating the Statement.

277. The Statement will be prepared, designated and published by the Secretary of State under new section 120E. The Statement will contain the government's strategic priorities relating to data protection (new section 120E(2)). This may include both domestic and international data protection priorities.

278. Under new section 120E(3), the publication of the Statement by the Secretary of State does not require a particular format.

279. New section 120F outlines the duties of the Commissioner in relation to the Statement.

280. Under new sections 120F(1-2), the Commissioner is required to have regard to the Statement. This means the Commissioner must consider the Statement when carrying out functions under data protection legislation. The Commissioner will not be required to consider the Statement when carrying out their functions in relation to a particular person, case or investigation. In particular, this means the Statement does not need to be taken into account when taking decisions on individual enforcement action.

281. New sections 120F(3-5) requires the Commissioner to respond, in writing, to the Statement to explain how the Commissioner will have regard to the statement and publish that response within 40 working days of the Statement's designation. This response is not required to take a particular form and it is envisaged that this obligation can be met by a standalone response to the Statement. The Secretary of State may extend the period for the Commissioner to provide a response under 120F(4)(b).

282. New section 120G outlines the review process for the Statement.

283. Under new sections 120G(1-3), when three years have elapsed since a Statement was first designated or when a review of the statement last took place, the Secretary of State must as soon as reasonably practicable review the existing Statement and, under section 120G(6), determine whether to amend it, leave it unchanged or withdraw it.

284. Under new section 120G(4), the Secretary of State may also review a designated Statement if a Parliamentary general election has taken place, or there has been a

significant change in the government's policy affecting data protection (within the meaning given in new section 120G(5)). New section 120G(4)(c) outlines that a further review may also take place on an amended statement that was not approved by Parliament.

285. If on a review of the statement, the Secretary of State decides to withdraw it, new section 120G(8) provides that the Secretary of State will be required to publish a withdrawal decision. The new section does not require this response to take a particular form.

286. New section 120G(7) clarifies that the same procedure for designating the first Statement applies to any subsequently amended Statements. This means a Statement can only be designated after the parliamentary approval procedure in section 120H and the Statement only has effect if designated under new section 120E.

287. Under new section 120G(9), the Secretary of State may make corrections to the Statement for clerical or typographical errors. These corrections will not be treated as amendments and will therefore not warrant parliamentary approval.

288. Under new section 120G(10), when a new Statement is designated, the previous Statement automatically ceases to have effect.

289. New section 120G(11) defines when a review of a statement is considered to have taken place.

290. New section 120H outlines the parliamentary procedure required before designating the Statement.

291. Under new sections 120H(1-2) a draft Statement prepared by the Secretary of State will be submitted to Parliament for approval via the negative resolution procedure on a non-amendable motion, which means the Statement can be rejected in full by either House of Parliament within a 40-day period. The Statement may not be designated until the end of this 40-day period. A Statement which has not received parliamentary approval cannot be designated.

292. New section 120H(4) is self-explanatory.

293. Clause 30 also inserts new subsection (1A)(c) into section 139 of the DPA 2018 requiring for the Commissioner to report how, in the relevant reporting period, they have had

regard to the Statement. This will be an additional part of the Commissioner's annual reporting requirements to Parliament under the DPA 2018 (see reporting to Parliament section 139 of the DPA 2018).

Clause 31: Codes of practice for the processing of personal data

294. Under sections 121 to 124 of the DPA 2018, the Commissioner is obliged to publish four statutory codes of practice. These codes are subject to a number of provisions within the DPA 2018; section 125 of the Act sets out the formal parliamentary approval process for the codes. Furthermore, these codes must be published and kept under review by virtue of the provisions set out in section 126 of the DPA 2018. According to the provisions under section 127, they are admissible in evidence in legal proceedings; ensuring that a court or tribunal, and the Commissioner, take any 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.

295. Section 128 allows the Secretary of State to make regulations requiring the

Commissioner to prepare other codes that give guidance as to good practice in the processing of personal data. Currently, codes made under section 128 do not follow the same parliamentary process set out in section 125, are not required to be published or reviewed as set out in section 126, and do not have the same legal effect set out in section 127 as those codes made under s121 - 124.

296. Clause 31 ensures that all codes of practice made by the Secretary of State (regardless of whether they are set out explicitly in the Act, or requested by the Secretary of State) follow the same parliamentary process and have the same legal effects.

297. To enable this in a structured and methodical manner, section 128 (Other codes of practice) has been repealed, and reinstated as a new section 124A, so that the provisions concerning the statutory process in making these codes and their legal effects follow on.

298. New section 124A provides the Secretary of State with the power to make regulations requiring the Commissioner to produce other codes of practice giving guidance as to good

practice in the processing of personal data. The regulations must describe the personal data or processing to which the code relates and may also describe the persons to which it relates. Before preparing the code, the Commissioner must consult any of those the Commissioner considers appropriate from the list at subsection (4). Such codes are to be required by regulations, which will be subject to the negative resolution procedure. In line with topic-specific codes set out in the DPA 2018, where ad-hoc codes made under new section 124A are in force, the Commissioner may prepare amendments of the code or a replacement code

299. Clause 31 (3) to (9) makes minor and consequential amendments to the DPA 2018, the Registration Service Act 1953, the Statistics and Registration Service Act 2007, and the DEA 2017 as a result of the repeal of section 128 of the DPA 2018 and replacement by new section 124A.

Clause 32: Codes of practice: panels and impact assessments

300. Clause 32 amends Part 5 of the DPA 2018 by inserting new sections 124B and 124C

which amend the procedures by which the Commissioner develops statutory codes of practice under sections 121 to 124 and new section 124A of the DPA 2018.

301. New section 124B outlines the requirement for the Commissioner to consult a panel of individuals when preparing a statutory code of practice, the process for establishing the panels and the arrangements the Commissioner should put in place on how the panel should conduct its activities. This is subject to new section 124B(11) which provides a power for the Secretary of State to make regulations to disapply or modify the new requirements for a panel to consider a code prepared under new section 124A of the DPA 2018.

302. New section 124B(2) requires the Commissioner to establish a panel of individuals to consider the code, and new section 124B(3) sets out requirements for the members of the panel. The panel must include individuals with expertise in the subject matter of the code and other individuals the Commissioner considers are likely to be affected by the code or their representatives. This may include, for example, government

officials; trade associations; representatives from relevant regulators, public authorities or industry bodies; and data subjects.

303. New section 124B(4) outlines the Commissioner's responsibilities before the panel considers the code. The Commissioner will be required to publish the draft code and a statement relating to the establishment of the panel including the members of the panel, process by which they were selected and reasons for their selection. The published statement under new section 124B(4)(b) does not need to take a particular form.

304. New section 124B(5) allows for a new panel member to be appointed by the Commissioner if a current panel member is not willing or able to serve on the panel. A member may leave the panel permanently or on a temporary basis e.g. because of illness. Under new section 124B(6), the Commissioner will be required to publish a statement, in no particular form, identifying the new member of the panel, the process of selection and the reasons for their selection.

305. New section 124B(7) is self-explanatory.

306. Under new section 124B(8), if the panel

submits a report on the code within the period determined, the Commissioner must make any changes to the draft code the Commissioner considers appropriate (which could be none) before publishing the draft code, the panel's response or a summary of it, and for instances where a recommendation by the panel has not been taken forward, the reasons for not doing so.

307. New section 124B(9) is self explanatory.

308. New section 124B(10) makes clear that the new requirements for a panel to consider the code also apply to amendments prepared in relation to the code.

309. New section 124B(11) provides a power for the Secretary of State to make regulations to disapply or modify the new requirements for a panel to consider the code in the case of a code which the Commissioner is required to prepare under new section 124A where specified in the regulations.

310. Under new section 124B(12), these regulations will be subject to parliamentary approval via the negative resolution procedure which means the regulation can be rejected in full by either House of Parliament.

311. New section 124C outlines the requirement for the Commissioner to conduct and publish impact assessments when preparing a code of practice under section 121 to 124A. This should include an assessment of who would be likely to be affected by the code and the likely effect the code will have on them.

Clause 33: Codes of practice: approval by the Secretary of State

312. Clause 33 inserts new section 124D into the DPA 2018 which provides for statutory codes of practice produced by the Commissioner to be approved by the Secretary of State before they are laid before Parliament.

313. These new provisions will apply to statutory codes of practice prepared under sections 121, 122, 123, 124 of the DPA 2018 and new section 124A. When a code is prepared under these sections, the Commissioner must submit the final version to the Secretary of State, as required by 124D(1).

314. New section 124D(2) provides that the Secretary of State has 40 working days to

decide whether to approve the code of practice. The definition of 40 working days is in new section 124D(8).

315. If the Secretary of State approves the code of practice, it must be laid before Parliament for parliamentary approval, as outlined at 124D(3).

316. New section 124D(4) outlines the requirements should the Secretary of State not approve a code of practice. The Secretary of State must provide a statement to the Commissioner which explains the reasons why the code has not been approved. For transparency, this statement must be published.

317. New section 124D(5) outlines the duties of the Commissioner if a code of practice is not approved. The Commissioner must revise the code in light of the statement provided by the Secretary of State. Under section 124D(6), the revised code must then be submitted to the Secretary of State, following which subsections 124(2-5) apply again.

318. New section 124D(7) is self-explanatory.

319. Clause 33 subsection (3) makes revisions

to section 125 of the DPA 2018 which sets out the process for approval by Parliament of codes prepared under section 121 to 124 and new 124A. These consequential amendments are necessary because the code must now be submitted to the Secretary of State for approval before it is laid before Parliament.

Clause 34: Vexatious or excessive requests made to the Information Commissioner

320. Clause 34 permits the Commissioner to charge a reasonable fee or refuse a request where the request is vexatious or excessive. This replaces the previous test (of whether the request was 'manifestly unfounded or excessive') and is consistent with the new test applying across the UK GDPR and DPA 2018.

321. This clause amends section 135 to make clear that the Commissioner may refuse to deal with a vexatious or excessive request made by any person.

322. Sections 134 and 135 confer separate powers to charge fees. Where a request is made (whether vexatious or excessive, or not), if section 134 is relevant, the Commissioner has the power to charge a reasonable fee under that section. If section 134 is not relevant (in particular, because the request comes from a data subject or data protection officer/senior responsible individual), the Commissioner may have the power to charge a reasonable fee under section 135. New subsection (1A)(a) has been included to

ensure that the powers to charge fees under section 134 and section 135 do not overlap.

323. Subsection (1A)(b) is included to ensure that the Commissioner's existing discretion to refuse to act where the Commissioner may be authorised, but not required to respond to a request, is preserved.

Clause 35: Analysis of performance

324. Clause 35 inserts new section 139A into the DPA 2018 which provides for the Commissioner to prepare and publish an analysis of the Commissioner's performance. This analysis should use key performance indicators to effectively measure the Commissioners' performance (see section 139A(1) and (3).

325. New section 139A(2) provides for this analysis to be published once a year at a minimum.

Enforcement

Clause 36: Power of the Commissioner to require documents

326. Clause 36 amends section 142

(information notices) of the DPA 2018 to clarify that the Commissioner can require specific documents as well as information when using the information notice power. This is a clarification of the Commissioner's existing powers.

327. Clause 36 subsections (3) to (7) make consequential amendments to references to information notices in section 143 (information notices: restrictions), section 145 (information orders), section 148 (destroying of falsifying information and documents), section 160 (guidance about regulatory action) and Schedule 17 (review of processing of personal data for the purposes of journalism). These amendments are needed as a result of the clarification to the information notice powers in section 142 and make clear that the relevant provision applies where documents are required under the information notice powers in the same way as for other information.

Clause 37: Power of the Commissioner to require a report

328. Clause 37 makes provision for the Commissioner to require a report on a specified matter when exercising the power under section 146 of the DPA 2018 to give an assessment notice.

329. Subsection (1) is self-explanatory.

330. Subsection (2) amends section 146 (assessment notices) of the DPA 2018.

331. Subsection (2)(a) inserts new subsections (j) and (k) in section 146 subsection (2) of the DPA 2018 requiring the controller or processor to make arrangements for an approved person to prepare a report on a specified matter and provide the report to the Commissioner.

332. Subsection (2)(b) inserts new section 3A after section 146 subsection (3) in the DPA 2018. This provides that the Commissioner may set out requirements in the assessment notice specifying how the report by the approved person is to be prepared, its content, form and when it is required to be completed by.

333. Subsection (2)(c) inserts new section 11A after section 146 subsection (11) in the DPA 2018. This requires the controller or processor

to pay the cost for this report, including the approved person's expenses.

334. Subsection (2)(d) adds a definition of an approved person to the terms defined in section 146 subsection (12).

335. Clause 37 amends section 146 (assessment notices) of the DPA 2018 by inserting new section 146(A). This outlines the process for approving the person preparing the report and makes clear that the decision to approve lies with the Commissioner.

336. Subsection (1) of new section 146A is self-explanatory.

337. Subsection (2) provides that the controller or processor is to nominate an approved person to prepare the report and that they are required to do so within the time set out by the Commissioner in the notice.

338. Subsection (3) provides that if the Commissioner is satisfied that the person nominated is suitable, that approval is to be provided to the controller or processor in writing.

339. Subsection (4) sets out the process to be followed if the Commissioner is not satisfied

that the person nominated is suitable. In such circumstances, the Commissioner is required to let the controller or processor know by written notice their decision, the reasons for their decision and the person the Commissioner is selecting to prepare the report.

340. Subsection (5) sets out the process if the controller or processor fails to nominate a person to prepare the report in the time specified in the notice. In such circumstances, the Commissioner will decide the person to prepare the report and must notify the controller or processor of that decision by written notice. The controller or processor is required to make arrangements for this and pay any associated costs, as would be the case if they had nominated the approved person.

341. Subsection (6) provides that the controller or processor is required to cooperate with the approved person in the process of preparing the report.

342. Clause 37 section (4) amends section 155 subsection (1) (penalty notices) of the DPA 2018 to allow the Commissioner to give a

monetary penalty notice where the Commissioner is satisfied that a person has failed to comply with the duty placed upon the controller or processor under new section 146A(6), to assist the approved person in preparing the report.

343. Clause 37 section (5) amends section 160 (guidance about regulatory action) in subsection (4) of the DPA 2018. This requires the Commissioner to include in the statutory guidance the factors the Commissioner will consider in deciding whether to issue an assessment notice requiring the preparation of a report, and the factors the Commissioner may take into account when determining the suitability of a person to prepare the report.

Clause 38: Interview notices

344. New section 148A makes provision about interview notices. An interview notice can be used to require a person to attend an interview and answer questions when required by the Commissioner.

345. Subsection (1) sets out when the power can be used.

346. Subsection (2) provides the Commissioner with a power to give an interview notice.

347. Subsection (3) makes provision about who an interview notice can be issued to.

348. Subsection (4) requires the Commissioner to specify where and when the interview will take place. This is subject to the restrictions in subsections (6) and (7).

349. Subsection (5) provides that the interview notice must explain the suspected infringement of the UK GDPR or DPA 2018 that is being investigated, consequences of non-compliance with the interview notice and information about how a person can appeal the notice.

350. Subsection (6) provides that an interview notice must not require the person to attend the interview before the end of the period in which an appeal could be brought.

351. Subsection (7) provides that if an appeal is brought, the person concerned need not comply with the interview notice until the appeal has been withdrawn or decided.

352. Subsection (8) provides that subsections (6) and (7) do not apply where the Commissioner considers there is an urgent

need for the interview and where the Commissioner provides reasons for the urgency. In these circumstances, however, the interview notice must provide at least 24 hours between the time of issuing the notice and when the person is required to attend the interview.

353. Subsection (9) is self-explanatory.

354. New section 148B places certain restrictions on the circumstances in which the Commissioner can require a person to answer questions under an interview notice.

355. Subsection (1) provides that an interview notice does not require a person to answer questions at interview to the extent that requiring the person to do so would involve an infringement of the privileges of either House of Parliament.

356. Subsections (2) and (3) provide that a person is not required to answer questions 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 under data protection legislation. .

357. Subsection (4) is self-explanatory.

358. Subsection (5) provides that an interview 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 under the DPA 2018 and the other offences listed in subsection (6).

359. Subsection (7) provides that a statement provided in response to an interview notice cannot be used as evidence in criminal proceedings brought under the DPA 2018 (except where the proceedings relate to the offence under new section 148C (false statements made in response to an interview notice)) unless in the proceedings the person gives evidence that is inconsistent with the statement, and evidence relating to the statement is put before the court by the person or a question relating to it is asked by the person or on their behalf.

360. Subsection (8) provides that an interview notice cannot be made in respect of personal data being processed for journalistic, academic, artistic or literary purposes.

361. Subsection (9) lists other bodies to whom the Commissioner cannot give an interview notice.

362. New section 148C (false statements made in response to interview notices) makes it an offence for a person to intentionally or recklessly make a false statement in response to an interview notice. This replicates the offence in section 144 of the 2018 Act.

363. Clause 38 subsection (3) amends section 149 (9)(b) of DPA 2018 (enforcement notices) to add interview notices to the regulation making powers in this section. This brings the interview notice function in line with assessment notices, information notices and penalty notices in this context.

364. Subsection (4) amends section 155 (1)(b) (penalty notices) of the DPA 2018 to include interview notices. Where the Commissioner is satisfied that a person has failed to comply with an interview notice, the Commissioner is permitted to give a monetary penalty notice requiring a person to pay the Commissioner an amount determined by the Commissioner.

365. Subsection (5) amends section 157 (4) (maximum amount of penalty) of the DPA 2018

to include interview notices. The maximum penalty amount in relation to failure to comply with an interview notice is the higher maximum amount. This provision brings the maximum amount of the penalty that may be imposed by a penalty notice for failure to comply with an interview notice in line with the maximum amount for existing enforcement powers. The higher maximum amount is defined in section 157 (5) of the DPA 2018.

366. Subsection (6)(a) amends section 160 (1) (guidance about regulatory action) to include interview notices in the functions for which the Commissioner is required to produce and publish statutory guidance. This brings the interview notice function in line with assessment notices, enforcement notices, information notices and penalty notices.

367. Subsection (6)(b) inserts new section 5A in section 160 and specifies the matters which the guidance must include in relation to interview notices.

368. Subsection (7) amends section 162 (rights of appeal) of the DPA 2018 to include an interview notice to the list of notices a person can appeal.

369. Subsection (8) amends section 164 (applications in respect of urgent notices) of the DPA 2018 to provide that the provisions for appealing an urgent notice apply to interview notices. This enables a person who is given an interview 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 with the notice.

370. Subsection (9) is self-explanatory.

371. Subsection (10) amends section 196 (penalties for offences) to provide that the offence provided for in section 148C (false statements made in responses to interview notices) is included in subsection (2). Section 196 (2) of the DPA 2018 sets out the maximum penalties for offences that can be tried summarily or on indictment. 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. This aligns the offence set out in section 148C with existing comparable offences in the DPA 2018,

including that in section 144 (false statements made in response to information notices).

372. Subsection (11) provides that "interview notice (Part 6)" is added to the terms defined in section 206 (index of defined expressions) in the DPA 2018 and signposts where the definition may be found in the DPA 2018.

373. Subsection (12) amends Schedule 17 (review of processing of personal data for the purposes of journalism) to insert new section 3A after paragraph 3 to make provision for where the Commissioner gives an interview notice during a review period. New section 148B(8) prevents the Commissioner from giving an interview notice with respect to the processing of personal data for the special purposes. Paragraph 3A of this Schedule will disapply section 148B(8), providing the Commissioner with the ability to give interview notices for the purpose of the review, but only where a determination under section 174 of the DPA 2018 has taken effect.

374. Subsection (12) also amends paragraph 4 of Schedule 17 to include interview notices. It applies section 164 of the DPA 2018

(applications in respect of urgent notices) to interview notices given under paragraph 3A.

Clause 39: Penalty notices

375. Clause 39 makes changes to the provisions for imposing penalties in Schedule 16 to the DPA 2018. Before issuing a penalty notice to a person, the Commissioner must inform the person of the intention to do so, by issuing a notice of intent. Paragraph 2 of Schedule 16 to the DPA 2018 currently provides that a penalty notice given in reliance on a notice of intent must be issued within 6 months from when the notice of intent is given. The amendments allow for the Commissioner to have more time to issue a final penalty notice after issuing a notice of intent where needed.

376. Clause 39 repeals paragraph 2(2) and (3) of Schedule 16 and inserts new sub-paragraph A1 and B1 into paragraph 4 of that Schedule. This provides for the Commissioner to give a penalty notice within 6 months of giving a notice of intent but allows the Commissioner to issue a penalty notice outside of the 6 month time limit if it is not reasonably practicable to issue a final penalty notice within this

timeframe. In such circumstances, the Commissioner would instead be required to issue a final penalty notice "as soon as reasonably practicable" after issuing the notice of intent. This allows the Commissioner to have sufficient time, after issuing a notice of intent, to consider oral or written representations and complete its investigations, where needed. This also places new requirements on the Commissioner to let the person know the outcome of its investigation by giving written notice where the Commissioner has decided not to give a penalty notice. This notice should also be given within 6 months of the day the notice is given or as soon as reasonably practicable thereafter.

377. Clause 39 introduces a new requirement to be included in section 160 of the DPA 2018. This requires the Commissioner to produce and publish guidance on the circumstances in which the Commissioner will need longer than 6 months to make a decision whether or not to issue a penalty notice.

Clause 40: Annual report on regulatory action

378. Clause 40 amends the DPA 2018 by

making provision for the Commissioner to annually publish a report detailing how it has discharged its regulatory functions.

379. Subsection 2 amends section 139 of the DPA 2018 by inserting new subsection 2A which allows the Commissioner to include their annual report on regulatory action in their general report which is laid before Parliament.

380. Subsection 4 inserts a new section 161A into the DPA 2018 outlining a report the Commissioner must produce and publish annually on the Commissioner's investigation and enforcement powers.

381. New section 161A(2) sets out the information that the annual report on regulatory action must include in relation to investigations on the application of the UK GDPR and enforcement powers exercised in relation to those investigations.

382. New section 161A(3) sets out the information the annual report on regulatory action must include on enforcement powers exercised in relation to law enforcement processing and intelligence services processing under Parts 3 and 4 of the DPA 2018.

383. New section 161A(4) provides that the Commissioner is required to produce and publish information about the number of penalty notices given in the reporting period that were given more than 6 months after the notice of intent was given under paragraph 2 of Schedule 16 and the reasons why that happened.

384. Under new section 161A(5) the report must summarise how the Commissioner has taken into account the Commissioner's own guidance on regulatory action while exercising the Commissioner's powers.

385. New section 161A(6) is self explanatory.

Clause 41: Complaints to controllers

386. Clause 41 inserts new sections 164A and 164B into the DPA 2018.

387. New section 164A outlines the procedures for dealing with complaints made by data subjects to data controllers.

388. New section 164A(1) outlines the right of a

data subject to complain to the data controller if the data subject considers that there is an infringement of their rights under the UK GDPR or Part 3 of the DPA 2018.

389. New section 164A(2) requires controllers to facilitate the making of complaints under this section by taking appropriate steps. This could include providing a complaint form to be completed electronically, or other appropriate means.

390. New section 164A(3) requires data controllers to acknowledge receipt of the complaint within a period of 30 days, beginning on the day the complaint is received.

391. New section 164A(4) requires data controllers to take appropriate steps to respond to the complaint and inform the complainant of the outcome of the complaint, without undue delay.

392. New section 164A(5) explains that the requirement in subsection(4)(a) for data controllers to “take appropriate steps to respond to the complaint” includes making enquiries about the subject matter of the complaint to the extent appropriate, and informing the complainant about the progress

of the complaint.

393. New section 164B sets out a power for the Secretary of State to make regulations to require controllers to notify the Commissioner of the number of complaints they have received in relation to the periods set out in regulations.

394. New sections 164B(2)-(5) set out further detail in relation to the regulations. Any such regulations must be made using the negative resolution procedure.

Clause 42: Power of the Commissioner to refuse to act on certain complaints

395. Clause 42 amends section 165 of the DPA 2018 and inserts new section 165A, which provides the Commissioner with a new power to refuse to act on data protection complaints if certain conditions are met. This power is in addition to the discretion that the Commissioner is already able to exercise under sections 165(4)(a) and (5)(a) respectively to take “appropriate steps” to respond to a complaint and to investigate the subject matter of a complaint “to the extent appropriate.”

396. New section 165A confers a power on the Commissioner to refuse to act on complaints if any of the conditions set out at subsections (2)-(4) of this section are met.

397. New section 165A(1) is self-explanatory.

398. New section 165A(2) sets out that the Commissioner may refuse to act on a complaint if that complaint has not been made to the controller under section 164A.

399. New section 165A(3) sets out that the Commissioner may refuse to act on a complaint if that complaint has been made to the controller under section 164A, but the controller has not finished handling the complaint in accordance with 164A(4), and the period of 45 days beginning with the day the complaint was made to the controller under that section has not expired.

400. New section 165A(4) sets out that the Commissioner may refuse to act on a complaint if the complaint is vexatious or excessive as set out in new section 204A.

401. New section 165A(5) is self-explanatory.

402. New section 165A(6) requires the Commissioner to inform the complainant of the

refusal, reasons for the refusal and the right to appeal against the refusal if the Commissioner refuses to act on a complaint under section 165.

403. New section 165A(7) is self-explanatory.

404. New section 165B outlines guidance that the Commissioner must produce about responding to and refusing to act on complaints.

405. New section 165B(1) requires the Commissioner to produce and publish guidance about how the Commissioner proposes to respond to complaints under section 165 (complaints by data subjects) and how the Commissioner proposes to exercise powers conferred by section 165A (power of the Commissioner to refuse to act on certain complaints).

406. New section 165B(2) provides that the Commissioner may alter or replace any guidance produced under this section, and requires that the Commissioner publish any altered or replacement guidance.

407. New section 165B(3) requires that the

Commissioner consult the Secretary of State as well as other such persons as the Commissioner considers appropriate before producing guidance under this section.

408. New section 165B(4) requires that guidance produced under this section is laid before Parliament.

409. Clause 42(5) inserts new section 166A into the DPA 2018 which deals with appeals against a refusal of the Commissioner to act on a data protection complaint.

410. New section 166A(1) provides that where the Commissioner refuses to act on a complaint in reliance on section 165A, the person who made the complaint may appeal to the Tribunal.

411. New section 166A(2) explains that the Tribunal may review any determination of fact on which the refusal to act was based.

412. New section 166A(3) explains that if the Tribunal considers that the refusal to act is not in accordance with the law or that the Commissioner ought not to have exercised the discretion to refuse to act, the Tribunal must allow the appeal.

413. New section 166A(4) explains that if the conditions under 166A(3) are not satisfied, the Tribunal must dismiss the appeal.

Clause 43: Complaints: minor and consequential amendments

414. Clause 43 introduces Schedule 8 containing miscellaneous minor and consequential amendments to the UK GDPR and the DPA 2018 relating to complaints by data subjects.

Clause 44: Consequential amendments to the EITSET Regulations

415. Schedule 2 of the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 S.I. 2016/696 ("the EITSET Regulations") currently applies (with appropriate modification) certain enforcement provisions contained within the DPA 2018, so that enforcement powers are available to the Commissioner as the supervisory body for trust service providers, in respect of breaches of Regulation (EU) No 910/2014 ("the eIDAS Regulation").

416. Clause 44 amends Schedule 2 of the EITSET Regulations in order to apply (with appropriate modification) the changes made by clauses 36, 37, 38, and 39 to current enforcement provisions within the DPA 2018, so that changes apply equally in respect of the Commissioner's enforcement powers, as the supervisory body for trust service providers.

417. Amongst amendments made by clause 44 to Schedule 2 of the EITSET Regulations, are amendments required in order to apply (with appropriate modification) the new enforcement power under section 146A of the DPA 2018, to require a technical report as part of the assessment notice procedure, and the new enforcement power under section 148A, to impose an interview notice to require a person to attend an interview and answer questions. The new offence of intentionally or recklessly making a false statement in response to an interview notice under section 148C is also applied by amendments made to Schedule 2 of the EITSET Regulations.

418. Clause 44 amends Schedule 2 of the EITSET Regulations, in order to remove the reference to consultation under section 65 of the DPA 2018 when section 155(3(c) is applied

with modification under Schedule 2 of the EITSET Regulations as the consultation requirements under that section are not relevant to the regulation of trust service providers under the UK eIDAS Regulation.

419. Clause 44 also amends Schedule 2 of the EITSET Regulations, in order to omit paragraph 21, which is a previous and unnecessary provision, given paragraph 1(y) of Schedule 2 only applies certain subsections of section 182 of the DPA 2018.

Protection of prohibitions, restrictions and data subject's rights

Clause 45: Protection of prohibitions, restrictions and data subject's rights

420. Clause 45(1) and (2) amend the 2018 Act by inserting a new section 183A into the DPA 2018. New section 183A creates a presumption in relation to the interaction between the data protection legislation and other legislative provisions or rules of law relating to the processing of personal data.

421. Subsection (1) of new section 183A sets out that any relevant enactment or rule of law providing a power or duty to process personal

data does not override any requirement imposed by the main data protection legislation, other than in the circumstances provided for in subsections (2) and (3). The reference to “enactment” includes devolved legislation. The “main data protection legislation” is defined in subsection 4.

422. Subsection (2)(a) of new section 183A ensures that subsection (1) does not apply to any enactments forming part of the main data protection legislation. Subsection (2)(b) recognises that there may be situations where legislation is deliberately intended to override requirements of the data protection legislation, and makes it clear that in such cases subsection (1) will not apply. This preserves the principle of parliamentary sovereignty. Whether or not devolved legislation is able to override the data protection legislation in this way will depend on the terms of the relevant devolution settlement.

423. Subsection (3) of new section 183A ensures that any duty or power in the legislation that makes provision for processing personal data can be taken into account for the purpose of determining whether it is possible to rely on any exception to a requirement in the

data protection legislation. For example, if there is a duty in legislation on a person or organisation to disclose personal data, the requirement for a lawful basis in Article 6(1) of the UK GDPR is likely to be met (Article 6(1)(c) provides a lawful basis for processing where the processing is necessary for compliance with a legal obligation to which the controller is subject).

424. Subsection (4) of new section 183A defines the relevant parts of the data protection legislation that constitute the "main data protection legislation" for the purposes of new s.183A(1). It also defines "relevant enactment" for the purposes of subsection (1) as meaning any enactment so far as passed or made on or after the day on which clause 45 of the Data Protection and Digital Information Bill comes into force. This limits the effect of subsection (1) to legislation passed or made on or after the day on which new section 183A comes into force. It also defines "requirement" as including a prohibition or restriction.

425. Subsection (5) of new section 183A confirms that the reference in subsection (1) to an enactment or rule of law that imposes a duty or confers a power to process personal

data includes duties or powers that arise directly or indirectly, for example: provisions that remove restrictions, or provisions that authorise a person to require another person to process personal data.

426. Clause 45(3) makes some amendments to section 186 of the DPA 2018 to clarify its intended application and effect, particularly in light of new section 183A. For example, new subsection 2A(b) of section 186 confirms the circumstances in which the rule set out in section 186 about the relationship between the relevant elements of the data protection legislation and other legislation can be disapplied in a way that mirrors subsection (2)(b) of new section 183A.

427. Clause 45(4) inserts a reference to new section 183A into section 5(A3)(a) of the European Union (Withdrawal) Act 2018, as amended by the Retained EU Law (Revocation and Reform) Act 2023. . This ensures that the interpretation rule relating to retained direct EU legislation made by new section 5(A2) of the European Union (Withdrawal) Act 2018, inserted by section 3(1) of the Retained EU Law (Revocation and Reform) Act 2023 I, is disapplied where new section 183A applies.

The UK GDPR constitutes retained direct EU legislation and therefore falls within the scope of new section 5(A2) of the European Union (Withdrawal) Act 2018.

Miscellaneous

Clause 46: Regulations under the UK GDPR

428. This clause makes provision concerning the form, process and procedure for making regulations under the powers in the UK GDPR, including consultation requirements. It makes it clear that, before making regulations, the Secretary of State must consult the Commissioner and such other persons as they consider 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.

Clause 47: Minor amendments

429. This clause introduces Schedule 9 containing miscellaneous minor amendments to the UK GDPR and the DPA 2018.

Part 2: Digital Verification Services

Introductory

Clause 48: Introductory

430. Clause 48 sets out the scope of Part 2 of the Bill and defines digital verification services (DVS).

DVS trust framework

Clause 49: DVS trust framework

431. Clause 49 subsections (1) to (3) require the Secretary of State to prepare and publish a DVS trust framework, and when preparing the framework to consult the Commissioner and any persons the Secretary of State thinks appropriate to consult. Subsection (4) sets out that this consultation can take place before clause 49 comes into force. Subsection (5) sets out that the trust framework should be reviewed at least every 12 months and in

consultation with the Commissioner and any persons the Secretary of State thinks appropriate to consult. Subsection (6) enables the Secretary of State to revise and republish the trust framework following a review, or at other suitable times.

432. Subsection (7) sets out that the trust framework or a revised version of the framework comes into force when it is published unless it specifies otherwise. Subsection (8) states that the trust framework or a revised version of the framework can come into force at different times for different purposes, and can include transitional or saving provisions.

DVS register

Clause 50: DVS register

433. Clause 50 subsections (1), (2) and (3) require the Secretary of State to establish and maintain a publicly available DVS register of organisations providing DVS. Subsections (4) and (5) provide that an organisation must be

registered if they hold a certificate issued by an accredited conformity assessment body confirming they are providing DVS in accordance with the DVS trust framework, they have applied to be registered, they have complied with the registration requirements under clause 51 and they have paid the relevant fee set under clause 52. As set out in clause 54 subsection (9), if an organisation applies to be re-registered during the specified period in which it has been removed from the register, the Secretary of State must refuse the application.

434. Subsection (6) ensures that where a certificate has expired or has been withdrawn or is a pre-revision certificate under clause 55 the organisation cannot be registered.

435. Subsection (7) is self-explanatory.

Clause 51: Applications for registration

436. Clause 51 subsection (1) enables the Secretary of State to determine the form in which an application for registration may be made, including the information and documents to be provided in support of an application. Subsection (2) sets out that a determination can make different provisions for

different purposes. Subsection (4) allows the Secretary of State to revise a determination about applications for registration. Subsections (3) and (5) require the Secretary of State to publish a determination or a revised determination under this section.

Clause 52: Fees for registration

437. Clause 52 subsection (1) and (3) enable the Secretary of State to make a determination requiring organisations to pay fees and for the determination to specify the amount to be paid. Subsections (2) and (4) provide that the fees can be set at a level higher than the administrative costs of determining an application for registration or the administrative costs associated with continued registration. Subsection (6) sets out that a determination can make different provisions for different purposes.

438. Subsection (5) provides that unpaid fees can be recovered summarily as a civil debt. Subsection (7) and (9) requires the Secretary of State to publish a determination or revised determination made under this section. A revised determination can be made by the Secretary of State under subsection (8).

Clause 53: Duty to remove person from DVS register

439. Clause 53 subsection (1) requires the Secretary of State to remove an organisation from the DVS register when the organisation asks to be removed, stops providing DVS or no longer holds a certificate from an accredited conformity assessment body. Subsection (2) provides that the duty to remove the organisation where the organisation no longer holds a certificate will apply where the certificate has expired, or has been withdrawn or is a pre-revision certificate under clause 55. Subsection (3) is self-explanatory.

Clause 54: Power to remove person from DVS register

440. Clause 54 subsection (1) enables the Secretary of State to remove an organisation from the DVS register if satisfied that the organisation is failing to comply with the DVS trust framework or has failed to provide information to the Secretary of State where a notice has been issued under clause 62.

441. Subsection (2) requires the Secretary of State to give written notice to the organisation

of an intention to remove them from the register. Subsection (3) sets out the information that must be included in a written notice. The notice must state the name and address of the recipient, the reasons for removal, the right to make written representations about the intention to remove them from the register, the date by which representations should be made and the period of the removal. Subsection (4) specifies that the organisation has a minimum of 21 days within which to make written representations to the Secretary of State.

442. Subsection (5) provides that the organisation can make oral representation if the Secretary of State deems this appropriate. The ability to make oral representations should be stated in the written notice and the notice must give the organisation details of how and when the oral representation can be made. Subsection (6) prohibits the organisation from being removed from the register before the deadline to make representations has passed.

443. Subsection (7) requires that any written or oral representations made in accordance with the written notice must be considered by the Secretary of State before a decision on

removal from the register is made.

444. Subsection (8) requires the Secretary of State to give written notice to an organisation informing them they have been removed from the register, and that any application to be re-registered during the period of removal specified in the notice must be refused. Subsection (9) requires the Secretary of State to refuse an application for re-registration during the period of removal specified in the notice. Subsection (10) sets out that the period of removal must start on the day the notice is given and not exceed two years.

Clause 55: Revising the DVS trust framework: top-up certificates

445. Subsection (1) specifies that this section applies when the Secretary of State revises and republishes the trust framework and a new rule is added or an existing rule is changed. Subsection (2) provides that where the trust framework rules are revised, the rules may specify that by a specified date an organisation holding a pre-revision certificate has to obtain a top-up certificate certifying they are providing DVS in accordance with the new rule. If they fail to do so, they will not be able to apply to be

registered in reliance on the pre-revision certificate and if they are already registered, they will be removed from the register.

446. Subsection (3) sets out the relevant definitions for this section.

Information Gateway

Clause 56: Power of public authority to disclose information to registered person

447. Clause 56 creates a permissive gateway enabling public authorities to share information relating to an individual with an organisation registered on the DVS register, where the individual makes a request to the registered organisation to provide DVS.

448. Subsection (3) sets out that information disclosed under this section does not breach any duty of confidentiality owed by the public authority making the disclosure or any other restrictions relating to the disclosure of information. Subsection (4) prohibits a public authority from disclosing information under this section that would breach data protection

legislation, although the power to disclose information under this section is to be taken into account in deciding whether the disclosure would breach data protection legislation. It also prohibits disclosure of information which is prohibited under Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016. Subsection (5) makes clear that public authorities may only disclose information which they have obtained through exercising functions of a public nature. Subsection (6) provides that this section does not override any existing powers to disclose information.

449. Subsection (7) enables public authorities to charge fees for disclosing information to organisations providing DVS. Subsection (8) is self-explanatory.

Clause 57: Information disclosed by the Revenue and Customs

450. Clause 57 applies to information disclosed by His Majesty's Revenue and Customs (HMRC) for the provision of DVS.

451. Subsection (2) sets out that the organisation providing DVS must not share information disclosed by HMRC for the

provision of DVS further without the consent of the Commissioners for HMRC.

452. Subsection (3) sets out that if a third party receives the information disclosed by HMRC to the DVS provider directly or by other means, the third party must not disclose the information without consent of the Commissioners for HMRC.

453. Subsection (4) sets out that the offence of wrongful disclosure under section 19 of the Commissioners for Revenue and Customs Act 2005 applies where information is disclosed in contravention of this section. Subsection (5) is self-explanatory.

Clause 58: Information disclosed by the Welsh Revenue Authority

454. Clause 58 applies to information disclosed by the Welsh Revenue Authority for the provision of DVS.

455. Subsection (2) sets out that the organisation providing DVS must not share information disclosed by the Welsh Revenue Authority for the provision of DVSfurther

without the consent of the Welsh Revenue Authority.

456. Subsection (3) sets out that if a third party receives the information disclosed by the Welsh Revenue Authority to the DVS provider directly or by other means, the third party must not disclose the information without consent of the Welsh Revenue Authority.

457. Subsection (4) sets out that it is an offence to disclose information in contravention of this section. Subsection (5) sets out the defences in relation to this offence - that the person charged with the offence reasonably believed that the disclosure of information was lawful, or that the information had already lawfully been made publicly available.

458. Subsection (6) sets out what punishments a person who commits an offence under subsection (4) will face. A person who commits the offence on summary conviction in England and Wales may be imprisoned for up to the maximum term available in a magistrates court, receive a fine, or both. A person committing the offence on summary conviction

in Scotland may be imprisoned for a term of up to 12 months, or receive a fine up to the statutory maximum, or both. A person who commits the offence on summary conviction in Northern Ireland may be imprisoned for up to 6 months, or receive a fine up to the statutory maximum, or both. In all UK jurisdictions, a person who is convicted of the offence on indictment may be imprisoned for up to 2 years or receive a fine, or both.

459. Subsection (7) is self-explanatory.

Clause 59: Information disclosed by Revenue Scotland

460. Clause 58 applies to information disclosed by Revenue Scotland for the provision of DVS.

461. Subsection (2) sets out that the organisation providing DVS must not share information disclosed by Revenue Scotland for the provision of DVS further without the consent of Revenue Scotland.

462. Subsection (3) sets out that if a third party receives the information disclosed by Revenue

Scotland to the DVS provider directly or by other means, the third party must not disclose the information without consent of Revenue Scotland.

463. Subsection (4) sets out that it is an offence to disclose information in contravention of this section. Subsection (5) sets out the defences in relation to this offence - that the person charged with the offence reasonably believed that the disclosure of information was lawful, or that the information had already lawfully been made publicly available.

464. Subsection (6) sets out what punishments a person who commits an offence under subsection (4) will face. A person who commits the offence on summary conviction in England and Wales may be imprisoned for up to the maximum term available in a magistrates court, receive a fine, or both. A person committing the offence on summary conviction in Scotland may be imprisoned for a term of up to 12 months, or receive a fine up to the statutory maximum, or both. A person who commits the offence on summary conviction in Northern Ireland may be imprisoned for up to 6

months, or receive a fine up to the statutory maximum, or both. In all UK jurisdictions, a person who is convicted of the offence on indictment may be imprisoned for up to 2 years or receive a fine, or both.

465. Subsection (7) is self-explanatory.

Clause 60: Code of practice about the disclosure of information

466. Clause 60 subsection (1) sets out that the Secretary of State must prepare and publish a code of practice regarding the disclosure of information under clause 56. Subsection (2) sets out that the code must be consistent with the data sharing code prepared and issued under the DPA 2018. Subsection (3) requires public authorities to have regard to the code of practice when disclosing information under clause 56.

467. Subsection (4) enables the Secretary of State to revise and republish the code of practice. Subsection (5) requires the Secretary of State to consult the Commissioner and any persons the Secretary of State thinks appropriate before preparing or revising the

code of practice. Subsection (6) states that the consultation exercise may be carried out before this Part comes into force.

468. Subsections (7) to (8) set out that the code of practice will be subject to approval by a resolution of both Houses of Parliament before it is first published, and subject to the negative resolution procedure for every republication.

469. Subsections (9), (10) and (11) are self-explanatory.

Trust mark

Clause 61: Trust mark for use by registered persons

470. Clause 61 provides that the Secretary of State can designate a trust mark to be used by organisations providing registered DVS. The Secretary of State must publish the trust mark. The trust mark cannot be used by organisations in the course of providing, or offering to provide, DVS unless they are registered in the DVS register. The Secretary of State can enforce unlawful use of the trust mark in civil proceedings.

Supplementary

Clause 62: Power of Secretary of State to require information

471. Clause 62 provides that the Secretary of State may by written notice ask accredited conformity assessment bodies and organisations included on the DVS register to provide information that the Secretary of State reasonably requires with respect to the exercise of the Secretary of State's functions under this Part.

472. Subsection (2) sets out that the written notice must explain why the information is required and subsection (3) makes further provision about the contents of the written notice. Subsection (4) makes clear that the written notice must provide information about the consequences of failing to comply with the notice.

473. Subsection (5) enables the Secretary of State to cancel a written notice under this section.

474. Subsection (6) sets out that the disclosure of information requested by the Secretary of State does not breach any duty of confidence

owed by the organisation disclosing information, or any other restriction on the disclosure of information.

475. Subsection (7) sets out that the disclosure of information requested by the Secretary of State must not infringe restrictions under clauses 57, 58 and 59 of this Part, data protection legislation or specified sections of the Investigatory Powers Act 2016.

476. Subsections (8) to (11) place certain limitations on the information which the Secretary of State may require the organisation to provide under a written notice .

Clause 63: Arrangements for third party to exercise functions

477. Clause 63 sets out that the Secretary of State may make arrangements for a person prescribed by regulations to exercise the functions of the Secretary of State under this Part.

478. Arrangements made under this section may provide for the Secretary of State to make payments to the person and for the circumstances in which those payments are to be repaid to the Secretary of State.

479. Regulations made under this section are subject to approval by a resolution from both Houses of Parliament.

Clause 64: Report on the operation of this Part

480. Clause 64 sets out that the Secretary of State must prepare and publish reports on the operation of this Part. The first report must be published within 12 months of section 49 coming into force and thereafter reports must not be published more than 12 months apart.

Part 3: Customer Data and Business Data

Clause 65: Customer data and business data

481. Clause 65 defines key terms and concepts for the regulation-making powers in Part 3.

482. Subsection (2) defines the terms “business data”, “customer data”, “data regulations”, “data holder”, and “trader”.

483. “Business” data is information about goods, services and digital content supplied or provided by the relevant trader. Without limitation, it may include information relevant to the availability or quality of the products or services the trader offers, for example, in a communications context, information which

enables a customer or prospective customer to determine a supplier's broadband coverage; information as to the trader's prices, to enable price comparison; and information about customer feedback.

484. "Customer data" is information relating to the customer of a trader: customer data could, for instance, include information on the customer's usage patterns and the price paid to aid personalised price comparisons.

485. A "data holder" is a trader or a person who, in the course of business, processes the data, as the customer's supplier might not necessarily hold the data themselves.

486. A "trader" is a person who supplies or provides goods, services or digital content in the course of a business whether acting personally or through another person. The concepts of "goods", "services", "digital content" reflect Part 1 (Consumer contracts for goods, digital content and services) of the Consumer Rights Act 2015.

487. Subsections (3) and (4) describe what is meant by a "customer". It covers persons who have at any time purchased or received goods, services or digital content from the trader

whether or not the customer has done so as a consumer or in the course of a business. "Customers" are intended to include consumers but also customers who are not individuals, such as corporate entities. To the extent that regulations apply to business customers, it is most likely that these will be small and medium-sized enterprises.

488. Subsection (5) is drafted on the basis that, in practice, data might not be transferred from one person to another; rather, it may be the case that the customer or authorised person is granted access to data which is, and remains, held by the data holder.

Clause 66: Power to make provision in connection with customer data

489. Clause 66 provides the principal regulation-making power in relation to customer data.

490. Subsection (1) enables the Secretary of State or the Treasury to make regulations requiring data holders to provide customer data either directly to a customer at their request or to a person authorised by the customer to receive the data, at the request of

the customer or the authorised person. It is envisaged that data will be provided to an authorised person rather than the customer since the authorised person will be best able to make use of the data on the customer's behalf (in the provision of innovative services such as account management services via a visual dashboard of accounts, displayed on a smartphone app) but the regulation-making powers have been kept broad to allow to allow for direct provision of data to customers in the future.

491. Subsection (2)(a) enables regulations to provide for the production, collection and retention of customer data so that data holders have specific data to hand in order to ensure that Smart Data schemes can operate consistently and effectively.

492. Subsection (2)(b) enables regulations to require or enable data holders to make changes to customer data if requested by the customer or an authorised person on behalf of the customer. This power is intended, in particular, to provide customers with rights to rectify data beyond the right to rectification in Article 16 of the UK GDPR which is limited to personal data and will therefore not cover all

customer data (for instance where a customer is not an individual).

493. Subsection (3) enables the Secretary of State or Treasury to make regulations to provide for an authorised person to be able to exercise the customer's rights in relation to the goods, services or digital content supplied or provided by the data holder. The intention is that this power might, for instance, be used to allow the authorised person to access and use the goods, services, or digital content in question, such as to make a payment from an account, or transact with the trader, such as to negotiate an improved deal, on the customer's behalf.

494. Subsection (4) requires that in deciding whether to make regulations for customer data, the Secretary of State or the Treasury must consider the effect of the regulations on customers, data holders, small and micro businesses, and on innovation in the supply of goods and products and competition.

Clause 67: Customer data: supplementary

495. Clause 67 outlines provisions that regulations relating to customer data may, among other things, contain. These provisions

are non-exhaustive.

496. Subsection (2) concerns requests for customer data including to identify circumstances where a data holder may or must refuse to act on a request. Without limitation, Smart Data schemes may impose requirements on how requests are to be made including security requirements and the regulations may contain provisions to ensure that data holders do not have to comply with requests in certain circumstances for instance in the case of unreasonable or excessive requests.

497. Subsection (3) concerns the procedures by which customers authorise a person to receive customer data on their behalf, or do other things such as to act on their behalf. Subsection (3)(a) and (b) provides for restrictions on persons which a customer may authorise to act on their behalf to those complying with conditions specified in the regulations and/or who are approved by a decision-maker (such as a sector regulator, or an industry-led body).

498. Subsection (4) concerns how customer data is to be provided and the customer's

rights may be exercised. Subsection (4)(a) envisages the provision of customer data on one or more occasions, for a specified period (e.g., continuously available for a set amount of time) or at specified intervals. Subsection (4)(b) envisages requirements for the use of specified facilities or services, including electronic communications services or Application Programme Interfaces (APIs). APIs are software intermediaries that allow two applications to talk to each other, e.g. share data and typically adhere to standards that are developer-friendly and easily accessible. Banks in scope of the CMA's Retail Banking Market Order were required to comply with APIs that were designed by a separate implementation body, to ensure the timely sharing of customer data.

499. Under Subsection (4)(c) and (d), the regulations may also require data holders to participate in or comply with arrangements for establishing, maintaining, or managing these facilities or services. For example, data holders may be required to participate in the design and implementation of mechanisms or protocols that allow for efficient and timely provision of data. Using the example of APIs,

data holders may be required to establish and maintain their APIs in alignment with standards prescribed or identified in the regulations.

500. Subsection (5) concerns provisions requiring or enabling data holders or authorised persons to produce, collect, or retain records of customer data provided in accordance with the regulations. Subsection (6) concerns the imposition of requirements on a person who processes customer data to assist a trader in complying with the regulations. Subsection (7) concerns the imposition of requirements relating to the processing of customer data.

501. Subsection (8) envisages provisions enabling or requiring a data holder or approved persons to publish specified information about customers' rights. Such provisions may be important, for instance, to require traders to draw customers' attention to their rights and how they may be exercised.

502. Subsection (9) concerns provisions for the making and handling of complaints. These complaints may originate from customers or authorised persons.

503. Subsection (10) concerns provisions for

dispute resolution. This may include appointing a person to determine disputes, with provisions about their powers when determining disputes, the effect of decisions relating to disputes, and provisions for the person to review their decisions and provisions for appeals to a court or tribunal. As an illustrative example, this 'person' may be a recognised ombudsman in a given sector, or simply an alternative dispute resolution (ADR) provider.

Clause 68: Power to make provision in connection with business data

504. Clause 68 provides the principal regulation-making power in relation to business data. While this is a distinct regulation-making power, it is envisaged to be used in conjunction with customer data regulations under clause 66.

505. Subsection (1) enables the Secretary of State or the Treasury to make regulations requiring data holders to provide business data to the customer or to third parties eligible to receive data under the regulations; the latter category of recipient should, in practice, include the authorised persons referred to in the context of clause 66 (1) although customer

authorisation is not required for the provision of business data. The regulations may, additionally or alternatively, require data holders to publish business data. This is because business data is likely to be data of a more “standard” kind that is not specific to a particular customer and it might be efficient to publish it in accordance with such arrangements as the regulations may prescribe.

506. Subsection (2) enables the Secretary of State or the Treasury to make regulations to provide for the production, collection and retention of business data. As with clause 66(2)(a), the purpose of this power is to require data holders to have specific data to hand in order to ensure that Smart Data schemes can operate consistently and effectively.

507. Subsection (3) mirrors subsection (4) clause 66 and requires that, in deciding whether to make regulations relating to business data, the Secretary of State or the Treasury considers the effect of the regulations on customers, data holders, small and micro businesses, and on innovation in the supply of goods and products and competition.

Clause 69: Business data: supplementary

508. Clause 69 outlines provisions that regulations relating to business data may, among other things, contain. These provisions are non-exhaustive. This clause largely mirrors clause 67 (provision of customer data: supplementary).

509. Subsection (2) concerns provisions about requests for business data including to identify circumstances where a data holder may or must refuse to act on a request to provide data, reflecting subsection (2) of clause 67.

510. Subsection (3) concerns provisions relating to approval of third party data recipients, whether in accordance with conditions specified in the regulations or a decision of a decision-maker.

511. Subsection (4) concerns provisions for how business data is to be provided or published reflecting, in relation to the provision of data, subsection (4) of clause 67.

512. Subsection (5) concerns provisions requiring or enabling data holders or authorised persons to produce, collect, or

retain records of business data, reflecting subsection (5) of clause 63.

513. Subsection (6) concerns the imposition of requirements on a person who processes business data to assist a trader in complying with the regulations, reflecting subsection (6) of clause 73.

514. Subsection (7) concerns the imposition of requirements relating to the processing of business data provided to a customer or another person, reflecting subsection (7) of clause 67.

515. Subsection (8) concerns provisions enabling or requiring a data holder or approved persons to publish specified information about customers' rights, reflecting subsection (8) of clause 67.

516. Subsection (9) concerns provisions for the making and handling of complaints, reflecting subsection (9) of clause 67.

517. Subsection (10) concerns provisions for dispute resolution, reflecting subsection (10) of clause 67.

Clause 70: Decision-makers

518. Clause 70 outlines provisions relating to decision makers that the regulations may, among other things, provide for. A decision-maker is a person on which clauses 67 (3)(b) and 69 (3)(b) confer the function of deciding whether a person other than a customer satisfies conditions enabling that person to access customer or business data or do other things such as to act on the customer's behalf, but decision-making functions may also be conferred in other contexts by virtue of clause 74(1)(g). The possible provisions listed in this clause are non-exhaustive. Decision-makers might (if they are a public body), or might not, be persons who are enforcers under clause 71 (enforcement of data regulations).

519. Subsection (2) allows the regulations to make provision about the appointment of the decision-maker.

520. Subsection (3) enables regulations to empower decision-makers to suspend or revoke decisions. In particular, it is anticipated that a decision-maker will have the power to suspend or revoke, in whole or in part, the eligibility of a person other than a customer to

access customer or business data or to act on a customer's behalf. It is possible that, instead of a full or partial suspension or revocation, a person's eligibility to receive data may be subject to conditions, or additional conditions, for instance to deal with a problem or risk identified (see clause 67 (3) and clause 69 (3)).

521. Subsection (4) provides for the conferral of powers on decision-makers to obtain information for the purpose of monitoring compliance with any conditions to which data recipients are subject under the regulations.

522. Subsection (5) clarifies that the powers referred to in subsection (4) include enabling a decision-maker to require the provision of information (but this is subject to clause 72).

523. Subsection (6) requires the regulations to make provision about the rights of persons affected by the exercise of decision-makers' functions including review of decisions and appeals to a court or tribunal. This provision is considered a necessary safeguard against a decision to revoke a person's eligibility to access data.

524. Subsection (7) provides for the regulations

to enable or require the publication of specified information relating to the exercise of a decision-maker's functions.

525. Subsection (8) allows the regulations to provide for a decision-maker to conduct its investigations through a third-party, and reflects clause 71 (10) in relation to enforcers.

526. Subsection (9) enables the appointment of multiple decision-makers and reflects clause 71 (11) in relation to enforcers.

527. Finally, subsection (10) allows the regulations to enable or require a decision-maker to publish guidance about how it intends to exercise its functions under the regulations.

Clause 71: Enforcement of data regulations

528. Clause 71 enables enforcement of the regulations by a public body specified in the regulations (an "enforcer").

529. Subsection (3) provides for powers of investigation to be conferred on an enforcer. This may include powers to require provision of information, and powers of entry, inspection, search and seizure. These powers are subject to the restrictions in clause 728 (restrictions on powers of investigation).

530. Subsection (4) provides for the regulations to enable an enforcer to issue a notice requiring compliance with the regulations (compliance notice), to provide for enforcement of compliance notices and to enable an enforcer to publish a statement that a person is not complying with the regulations or with a compliance notice allowing the enforcer to name organisations which do not comply.

531. Subsection (5) enables the regulations to create offences punishable with a fine in cases where a person provides false or misleading information to the enforcer, or an act of omission which prevents an enforcer from accessing information, documents, equipment, or other material.

532. Subsection (6) enables the regulations to allow an enforcer to impose financial penalties in the case of provision of false or misleading information in the course of an investigation, or a failure to comply with a requirement imposed by the regulations or compliance notice. These powers are subject to the restrictions in clause 73 (financial penalties).

533. Subsection (7) enables the provision of

rights for people affected by the enforcer's actions under the regulations (for instance data holders) including provisions to review the decisions made by an enforcer and provision about appeals to a court or tribunal. In addition, there are specific and mandatory safeguards in the case of financial penalties: see clause 73.

534. Subsection (8) enables the regulations to make provision about complaints, including requiring enforcers to implement procedures for the handling of complaints.

535. Subsection (9) enables the regulations to require an enforcer to publish, or provide to a specific person, specified information relating to the enforcement of the regulations. This may include information about activities undertaken by the enforcer of its functions, either generally or specific to a particular case, and information about convictions for offences.

536. Subsection (10) enables enforcers' powers of investigation to be carried out by another person (which reflects the investigatory powers in relation to consumer law in Schedule 5 to the Consumer Rights Act 2015).

537. Subsection (11) provides for the

appointment of multiple enforcers. Where this is the case, regulations may appoint a "lead" enforcer. Other enforcers may be required to consult the lead before exercising their functions, and the lead may issue directions as to which enforcer may exercise a function in a particular case.

538. Finally, subsection (12) allows the regulations to enable or require an enforcer to publish guidance about how it intends to exercise its functions under the regulations.

Clause 72: Restrictions on powers of investigation etc

539. Clause 72 restricts the potential of powers of investigation provided for in Clause 67. Subsection (1)(a) ensures regulations may not authorise entry of an enforcer to a private dwelling without a court-issued warrant.

540. Subsection (1)(b) requires that regulations may not require a person to give an enforcer information to which subsections (2) to (7) apply. This information consists of information:

- the provision of which would infringe the privileges of Parliament (subsection (2));
- in respect of a communication between a

professional legal adviser and the adviser's client and in connection with legal advice to the client regarding the regulations (subsections (3) and (5));

- in respect of a communication between a professional legal adviser and the adviser's client or another person, in connection with proceeding arising out of the regulations, and for the purpose of any such proceedings (subsections (4) and (5));
- the provision of which would expose a person to prosecution for an offence other than an offence under the regulations or other legislation listed in subsection (7) (subsections (6) and (7)).

541. Subsection (8) prevents an oral or written statement given in response to a request for information from a decision-maker or an enforcer being used in evidence against the person being prosecuted for an offence, other than an offence created by the data regulations, subject to the exceptions in paragraphs (a) and (b).

Clause 73: Financial penalties

542. Clause 73 makes provision in relation to

financial penalties and imposes safeguards as to their use.

543. Subsection (2) requires that the amount of a financial penalty must be specified in, or determined in accordance with, the regulations. For example, the regulations may set a maximum limit of the value of a financial penalty that is to be imposed by an enforcer and the methodology that must be used to determine a specific financial penalty.

544. Under subsection (3)(a), the regulations must require an enforcer to issue, and then have regard to, guidance about how the enforcer will determine the amount of a financial penalty where it has discretion as to the amount of the penalty.

545. Under subsection (3)(b), an enforcer must provide the person on which a financial penalty is to be imposed with a written notice of the proposed financial penalty in advance of imposing it ("a notice of intent").

546. Under subsection (3)(c) and (d), an enforcer must provide the person on which a financial penalty is to be imposed with an opportunity to make representations about the proposed financial penalty. For example, the

regulations may provide the opportunity to submit an official statement to the enforcer before it makes a decision.

547. Under subsection (3)(e), if the enforcer proceeds with imposing a financial penalty, the enforcer must issue a final written notice to the person on which the penalty is being imposed.

548. Subsection (3)(f) to (g) requires that the regulations provide the person on which the penalty is imposed with a right of appeal and the regulations must specify the powers of the court or tribunal on such an appeal (this includes, for example, whether the court may substitute the enforcer's decision with its own or remit the decision to be retaken by the enforcer).

549. Subsection (4) provides that the regulations may:

- make provisions for a notice of intent or final notice to be withdrawn or amended, for example if the circumstances change (paragraph (a));
- set out circumstances under which the enforcer is required to withdraw a final notice (paragraph (b));

- in the case of a late payment, increase a financial penalty by a specific amount or determined in accordance with the regulations (paragraph (c));
- make provision as to how financial penalties are recoverable (paragraph (d)).

Clause 74: Fees

550. Subsection (1) of clause 74, enables the regulations to allow persons in subsection (2) to require the payment of fees by persons to which subsection (3) applies for the purpose of meeting expenses incurred in consequence of the regulations. The regulations may also make provision as to how the monies received must or may be used.

551. Subsection (2) lists the persons who the regulations may permit to charge fees. It is mainly intended that fees may be charged by decision-makers, enforcers and any other persons carrying out functions in consequence of the regulations but subsection (2) also allows fees to be charged by data holders (who might, for instance, be allowed to charges fees in the case of excessive requests for data). There are no provisions on the charging of fees by authorised persons as the

basis of the arrangements between authorised persons and customers is a commercial matter for them to determine.

552. Subsection (3)(a) provides that the regulations may only provide for payment of fees by persons who are directly affected by the performance of duties, or exercise of powers, under the regulations. This would include data holders, customers and authorised persons. Subsection (3)(b) provides that the amount of the fee may exceed the cost in respect of which it is charged. This is intended to allow for fees of a standardised amount, reflecting a general, or generally anticipated, cost of performance of functions of a particular kind, as opposed to costs incurred in a specific case, in the interests of the efficiency and effectiveness of a scheme.

553. Subsection (4) ensures the regulations must provide for the amount of a fee to be either specified in the regulations or determined in accordance with the regulations, or not to exceed such an amount.

554. Subsection (5) allows regulations specifying an amount, or maximum amount, of a fee to allow fees to increase at times and

amounts determined in accordance with the regulations for instance to cater for inflation.

555. Subsection (6) provides that where a person is given discretion to determine the amount of the fee, that person must publish information about the amount and how it is determined.

556. Subsection (7) allows the regulations to make provision about interest on, and recovery of, unpaid sums. This is intended to ensure that interest can be charged, and payments can be collected, in the event that those to whom the charge is applied do not pay on time.

Clause 75: Levy

557. Clause 75 under subsection (1), enables the regulations to impose, or (subject to subsection (3)) provide for a specified public body to impose, a levy on data holders. The purpose of the levy is to meet all or part of the costs incurred by enforcers and decision-makers or persons acting on their behalf. The intention is to ensure that expenses are met by the relevant sector without incurring a cost to the taxpayer. Subsection (1)(b) allows the regulations to specify how levy funds must or

may be used.

558. Subsection (2) requires that any levy may only be imposed in respect of data holders that appear to be capable of being directly affected by the exercise of the functions conferred on decision-makers and enforcers.

559. Subsection (3) ensures that, where regulations provide for a levy to be imposed by a specified public body, the regulations must specify how the rate of a levy is to be determined, how the period when the levy is payable is to be determined and require the public body concerned to publish information about the rate and period and how they are determined.

560. Subsection (4) allows the regulations to make provision about interest on, and recovery of, unpaid sums. This will ensure that interest can be charged, and payments can be collected effectively, in the event that those to whom the levy applies do not pay on time.

Clause 76: Financial assistance

561. Clause 76 provides statutory authority for the Secretary of State or the Treasury to give financial assistance to decision-makers or

enforcers for the purpose of meeting any expenses in the exercise of their functions. Under subsection (2), the assistance may be given on terms and conditions that the regulation-maker deems appropriate.

562. Subsection (3) defines "financial assistance" as any kind of financial assistance whether actual or contingent, including a grant, loan, guarantee or indemnity but does not include the purchase of shares.

563. It is intended that Smart Data schemes will be "self-financing" (through the fees and levies provided for by clause 74 and 75 but it is deemed appropriate for there to be a statutory spending authority as a "backstop" provision if that is necessary.

Clause 77: Confidentiality and data protection

564. Clause 77 subsection (1) ensures that regulations may not impose or confer a duty or power requiring or authorising processing of information that would breach an obligation of confidence (paragraph (a)), contravene the data protection legislation (paragraph (b)), or contravene another enactment of the law (paragraph (c)).

565. Subsection (2) provides that the regulations are not to be read as authorising processing of personal data that would contravene the data protection legislation but also provides that, in determining whether processing of data would do so, account may be taken of any power conferred or duty imposed by the regulations. The requirements of subsections (1) and (2) reflect section 238B(6) and (7) of the Pension Act 2004 relating to pensions dashboards.

Clause 78: Regulations under this Part

566. Clause 78 subsection (1) provides for supplemental matters. In particular, paragraph (f) allows the regulations to make provision by reference to specifications or technical requirements published from time to time by a specified person. This power reflects section 238A(5)(a) of the Pensions Act 2004 relating to pensions dashboards and is essential to enable effective and secure provisions envisaged in clause 67 (4)(b) and clause 69 (4)(b) for instance relating to APIs which will necessarily require regular change in light of developments of information technology.

567. Subsection (2) allows for the amendment,

repeal or modification of the application of primary legislation (see subsection (6)) in limited circumstances, these being: provision about handling of complaints; provisions about dispute resolution; incidental, supplementary, consequential, transitional or saving provisions (see subsection (1)(g)). It is envisaged that this power might, for instance, be used to extend any statutory dispute resolution scheme relating to a specific sector to any Smart Data scheme which applies to that sector.

568. Subsection (3) specifies the circumstances in which regulations must be subject to affirmative Parliamentary scrutiny. This is the case for the first regulations under clause 66(1)-(3) and 70(1) and (2) making provision about a particular description of customer data or business data (paragraphs (a) and (b)): the intention is that any regulations introducing a Smart Data scheme will be subject to affirmative scrutiny. Affirmative scrutiny is also required where regulations make requirements more onerous for data holders (paragraph (c)), where the regulations confer enforcement functions or make provisions for fees or a levy (paragraph (d)) and in case of any modification of primary legislation (paragraph (d)).

569. Subsection (5) requires that before making regulations of the kind requiring affirmative resolution, the Secretary of State or the Treasury must, as they consider appropriate, consult:

- persons likely to be affected the regulations e.g., businesses who would become data holders under the regulations;
- sectoral regulators with functions in relation to data holders under the proposed regulations.

570. Neither the consultation obligation in subsection (5) nor anything else in Part 3 affects the obligation of the Secretary of State to consult the Information Commissioner under Article 36.4 of the UK GDPR, where it applies.

Clause 79: Duty to review regulations

571. Clause 79 subsection (1) requires the Secretary of State or the Treasury to review regulations at least at five-yearly intervals. This provision is designed to align with reviews under sections 28 to 32 (secondary legislation: duty to review) of the Small Business, Enterprise and Employment Act 2015 where it

applies.

572. Subsection (2) requires that the reviewer must have regard to the matters the regulation-maker is required to consider in determining whether to make regulations under clause 66(4) and clause 70(3).

573. Subsections (3) to (5) requires publication of a report setting out the findings of the review, in which information can be omitted from publication if to do so would contravene the data protection legislation or harm the commercial interests of any person. The reviewer must arrange for a copy of any review report to be laid before Parliament.

Clause 80: Repeal of provisions relating to supply of customer data

574. Clause 80 repeals sections 89 to 91 (supply of customer data) of the Enterprise and Regulatory Reform Act 2013 which these clauses replace.

Clause 81: Interpretation of this Part

575. Clause 81 defines, or refers to the definition of, various terms used in these clauses.

Part 4: Other Provision about Digital Information

Privacy and electronic communications

Clause 82: The PEC Regulations

576. Clause 82 defines the meaning of "the PEC Regulations". This term is used in sections 83 to 92 of this Act.

Clause 83: Storing information in the terminal equipment of a subscriber or user

577. Current regulation 6 of the PEC Regulations sets out rules on the confidentiality of "terminal equipment" such as computers, mobile phones, wearable technology, smart TVs and connected devices, including the Internet of Things. Regulation 6(1) prohibits an organisation from storing information or gaining access to information stored in the terminal equipment of an individual, unless the individual is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and the individual has given consent. These rules apply to the placement of cookies and similar technologies (such as tracking pixels) on people's devices.

578. In this explanatory note, where the term “cookie” or “cookies” is used, this should be understood as referring to both cookies and similar technologies; and where the term “device” is used, this refers to “terminal equipment”.

579. Clause 83 (2)(a) amends regulation 6 of the PEC Regulations. It introduces new exceptions to the consent requirement in regulation 6(1) for certain purposes that are considered to present a low risk to people’s privacy. These exceptions are set out in new paragraphs (2A), (2B), (2C) and (2D).

580. Clause 83 (2)(a) also substitutes the current paragraph 6(1) with a new paragraph which makes it clear that the regulation applies to the storing of information on a person’s device as well as the access of information on a person’s device. The new paragraph 6(1) of the PEC Regulations also contains consequential amendments to refer to the new exceptions to the consent requirement. Clause 83 (2)(a) also substitutes paragraph 6(2) of the PEC Regulations, making minor changes to the language of that paragraph.

581. New paragraph (2A) introduces the first

new exception to the consent requirement. The exception permits the storage of information, or access to information, for the purpose of collecting statistical information about how an organisation's information society service is used, with a view to making improvements to that service. For example, statistical information showing how many people are accessing a service, what they are clicking on and for how long they are staying on a particular web page. Sub-paragraph (2A)(c) provides a safeguard that prevents onward sharing of information except where the sharing is for the purpose of making improvements to the service or website concerned. The exception applies only where the user is provided with clear and comprehensive information about the purpose and is given a simple and free means of objecting to the storage or access.

582. New paragraph (2B)(b)(i) introduces a new exception to the consent requirement, for the purpose of enabling the way an information society service ("ISS") appears or functions when displayed on a subscriber or user's device, to adapt to the preferences of that subscriber or user - for example, their font

preferences. Paragraph (2B)(b)(ii) removes the consent requirement for the purpose of enabling an enhancement of the appearance or functionality of an ISS when displayed on a user's device. This could be, for instance, where a cookie identifies performance-related information which can be used to optimise content, for example "responsive design" which enables a webpage to reconfigure itself for the particular dimensions of a monitor or screen. Paragraphs (2B)(c) and (d) provide that the exception applies only where the subscriber or user is provided with clear and comprehensive information about the purpose and is given a simple and free means of objecting to the storage or access.

583. New paragraph (2C) removes the consent requirement for the purpose of enabling the installation of software updates on a subscriber or user's device that are necessary for security reasons, subject to certain conditions set out in sub-paragraphs (a) to (e). In particular, users should be given the opportunity to postpone the update before it takes effect.

584. New paragraph (2D) removes the consent requirement where the sole purpose is to enable the geographical position of a

subscriber or user to be ascertained so that assistance can be provided in response to the user or subscriber's emergency communication from their terminal equipment. Current paragraph (3) of regulation 6 of the PEC Regulations provides that, where an organisation stores or accesses information in the terminal equipment of a subscriber or user on more than one occasion, it is sufficient for the purposes of regulation 6 that the requirements of paragraph (2) are met in respect of the initial use.

585. Clause 83 (2)(b)(ii) (b) and (c) contains consequential amendments to paragraph (3) to refer to the new exceptions to the consent requirement - specifically (2A) and (2B).

586. Current paragraph (3A) of regulation 6 of the PEC Regulations provides that, for the purposes of current paragraph 2, people may signify consent or objection via controls on their internet browser, or controls on other applications or programmes. Clause 83 (2)(c) makes some minor, clarificatory language changes to paragraph 3A, and some consequential amendments, to reflect the new purposes for which the consent requirement is being removed.

587. Clause 83 (2)(d) inserts new paragraphs 5, 6 and 7 into regulation 6 of the PEC Regulations.

588. New paragraph 5 provides a non-exhaustive list of examples of “strictly necessary” purposes for the purpose of 6(4)(b) of the PEC Regulations.

589. New paragraph 6(a) clarifies that a reference to an organisation storing information, or gaining access to information stored, in the device of a subscriber or user, includes a reference to the person instigating the storage or access.

590. New paragraph 6(b) clarifies that, a reference, except in paragraph (2A), to gaining access to information stored in the terminal equipment of a subscriber or user includes a reference to collecting or monitoring information automatically emitted by the terminal equipment (“emissions data”). An example of emissions data includes wifi probe requests.

591. New paragraph 7 is self-explanatory.

592. Clause 83 (3) inserts two new regulations into the PEC Regulations: regulation 6A and

regulation 6B.

593. New regulation 6A introduces at 6A(1)(a), a power for the Secretary of State (SoS) to add new exceptions to the cookie consent requirements. The power would also allow the SoS to omit or vary any existing exceptions to the consent requirements.

594. Paragraph (1)(b) of new regulation 6A provides that the SoS can also make consequential, supplementary, incidental, transitional, transitory or saving provisions which are necessary to give effect to exceptions made by regulations made under these provisions.

595. Paragraph (3) of new regulation 6A provides that, before making regulations under paragraph 6A(1), the Secretary of State must consult the Commissioner and "such other persons as the Secretary of State considers appropriate".

596. Paragraph (4) of new regulation 6A provides that the regulations made under this power are subject to the affirmative resolution procedure.

597. Regulation 6B introduces a power for the

SoS to make regulations providing that relevant organisations, for example, browser and device suppliers, may not supply "information technology of a specified description" unless it meets the requirements specified in the regulations. The purpose of regulation 6B is to ensure sufficient availability of technology which enables subscribers or users to effectively express their consent preferences.

598. Paragraph (3) of new regulation 6B provides that regulations made under this power may confer functions on the Commissioner relating to their enforcement.

599. Paragraph (4) of new regulation 6B defines "information technology". The definition is intended to be broad and future-proofed so all relevant technology that allows people to manage their consent preferences is included.

600. Paragraph (5) of new regulation 6B provides that the SoS can also make consequential, supplementary, incidental, transitional, transitory or saving provisions amending the regulations made under this power.

601. Paragraph (6) of new regulation 6B

provides that, before making regulations under paragraph 6B(1), the Secretary of State must consult the Commissioner, the Competition and Markets Authority and "such other persons as the Secretary of State considers appropriate".

602. Paragraph (7) of new regulation 6B provides that the regulations made under this power are subject to the affirmative resolution procedure.

603. Paragraph (8) of new regulation 6B sets out the meaning of key terms within the provision.

Clause 84: Unreceived communications

604. Clause 84 enables the Commissioner to investigate and take action against organisations which are responsible for generating unsolicited direct marketing communications, regardless of whether they are received by the intended recipient.

605. Clause 84 (2) amends the definition of "calls" in Regulation 2(1) to make it clear it includes all calls, whether or not they connect with the intended recipient. It also amends the definition of 'communication' to make it clear it

covers communications, such as texts and emails, which are “transmitted”. Previously the regulation only referred to communications that were “exchanged or conveyed”, which implied they needed to reach their intended recipient.

606. Clause 84 (3) inserts paragraph (1A) in Regulation 2. Paragraph (1A) clarifies the meaning of ‘recipient’ in the context of calls or communications that are sent or generated but not received. It provides that in this context, a reference in the Regulations to a recipient should be taken to mean the ‘intended recipient’.

Clause 85: Meaning of “direct marketing”

607. The Privacy and Electronic Communications (EC Directive) Regulations 2003 draws its definition of direct marketing from the Data Protection Act 2018.

608. This technical amendment does not change the definition of direct marketing, but places it directly into PEC Regulation 2(1) to aid readability of the legislation.

Clause 86: Use of electronic mail for direct marketing purposes

609. Clause 86 adds a new provision to PEC Regulation 22 so that non-commercial organisations will be treated the same as commercial organisations in respect of the so-called ‘soft opt-in’ rule. Under that rule, commercial organisations can send electronic marketing communications, such as emails and texts, to a person without consent if their contact details were collected during the sale of a product or service, or negotiations of a sale. Additional safeguards ensure that subsequent marketing communications with the customer must be in relation to similar goods and services and the person must also be offered a simple means of opting out of receiving further communications.

610. Clause 86 (3) adds a new subsection (3A) to regulation 22. Subsection (3A)(a) permits organisations which have charitable, political or non-commercial objectives to send electronic marketing communications for the purposes of furthering their objective.

611. Subsection (3A)(b) provides that the contact details of the recipient must have been obtained from the individual in the course of that person expressing an interest or providing support for the objectives of the organisation.

612. Subsection (3A)(c) provides that the individual must be given a simple way of opting out of receiving communications at the point their data was initially collected and at each subsequent communication.

Clause 87: Direct marketing for the purposes of democratic engagement

613. Clause 87 (1) provides that the Secretary of State may make exceptions from the direct marketing provisions in the PEC Regulations for communications carried out for the purposes of democratic engagement, providing electronic communications are not directed at individuals under the age of 14. This reflects the variations in voting age across the nation, where in some parts of the UK, such as Scotland, a person can register to vote at the age of 14 as an attainer.

614. Clause 87 (2) sets out the organisations and individuals that can rely on any exceptions created by these regulations and in what circumstances.

615. Clause 87 (3) provides that any exceptions introduced by regulations under this section may be subject to conditions and limitations.

616. Clause 87 (4) provides that regulations made under this section may make any consequential, supplementary, incidental, transitional, transitory or saving provisions.

617. Clause 87 (5) provides that the Secretary of State must consult the Commissioner and other persons she considers appropriate before making regulations.

618. Clause 87 (6) provides that the Secretary of State must consider the privacy of individuals before making regulations.

619. Clause 87 (7) sets out the parliamentary approval process which will apply to any regulations made under this section

Clause 88: Meaning of expressions in section 87

620. Clause 88 explains the key expressions and definitions used in clause 87. Subsections (1) - (5) are self-explanatory.

Clause 89: Duty to notify the Commissioner of unlawful direct marketing

621. Clause 89 introduces the new regulations 26A-C to the PEC Regulations. These regulations place a duty on public electronic communication service and public electronic

communication network providers to report suspicious activity relating to unlawful direct marketing activity to the Information Commissioner; set out the penalties for non-compliance; and requires the Commissioner to publish guidance on what might constitute reasonable suspicions.

622. Regulations 26A(1) and 26A(2) provide that the duty will apply to service and network providers who have reasonable grounds for suspecting that a breach of PEC Regulations might be occurring. An example of this might be where a high number of calls originating from one or a batch of numbers within a very short space of time are made to private telephone numbers in sequence. This could indicate speculative, unsolicited marketing calls being made. The network or service provider will not be required to intercept or examine the content of the communication. Regulation 26A(3) provides that relevant suspicions should be reported to the Commissioner within 28 days of the network or service provider first becoming aware of such activity. Regulation 26A(4) provides that this duty applies to network and service providers in respect of suspicious activity which is likely

to be in breach of direct marketing rules under PEC Regulations 19-22.

623. Regulations 26B(1) and (2) set out the circumstances in which the Commissioner can impose a fixed penalty on service or network providers of £1,000. Regulations 26B(3) to (7) set out the procedures the Commissioner must follow for issuing notices of intent to impose a fixed penalty and imposing penalty notices. Regulations 26B(8) provides network and service providers with the right to appeal the fixed penalty. Regulations 26B(9) provides that any fines collected must be paid into the Consolidated Fund; and Regulations 26B(10) to (12) set out the procedures for enforcing collection of unpaid fines in the courts where necessary. Regulations 26B(13), (14) and (16) provide that the Secretary of State may adjust the fixed monetary penalty amount by laying a statutory instrument in Parliament, which is subject to the affirmative resolution procedure. Regulations 26B (15) provides that, before making regulations under regulation 26B(13), the Secretary of State must consult the Commissioner and "such other persons as the Secretary of State considers appropriate".

624. Regulation 26C(1) requires the

Commissioner to publish guidance for the telecoms companies on what might constitute "reasonable grounds" for suspecting an individual or organisation being responsible for unlawful direct marketing activity.

625. Regulation 26C(2) provides that the Commissioner can alter and replace the guidance when required and must publish the altered or replacement guidance. Regulation 26C(3) requires the Commissioner to consult with Ofcom (the telecommunications regulator), the telecoms companies, the Secretary of State and any other interested parties before the guidance is produced. Regulation 26C(4) requires the Commissioner to refer to the guidance before determining whether to issue a fixed penalty notice under regulation 26B. Regulation 26C(5) defines the meaning of 'Direct marketing regulations'.

626. Clause 89(3) makes amendments to Regulation 5C of the PEC Regulation to ensure consistency with Regulations 26B(10) to (12).

627. Clause 89(4) inserts a new regulation into the PEC Regulations: regulation 18A. This regulation introduces the regulations dealing

with direct marketing in the PEC Regulations and cross-refers to the regulation-making power in Clause 87 of the Bill.

Clause 90: Commissioner's enforcement powers

628. The Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PEC Regulations') set out privacy rights relating to electronic communications.

629. Clause 90 updates the PEC Regulations enforcement powers which currently rely on powers in the DPA 1998. The effect of clause 86 will be to apply some of the more modern enforcement provisions in the DPA 2018 to the PEC Regulations enforcement regime.

630. Clause 90 (2) and (3) omit paragraph 6 of regulation 5 and paragraph 5B of the PEC Regulations, which are both concerned with the Commissioner's powers to audit measures taken by public electronic communications service providers to safeguard the security of their services and inform certain parties of a personal data breach. These provisions are no longer needed as section 146 of the DPA 2018 (powers for the Commissioner to impose assessment notices) will instead be applied for the purposes of the PEC Regulations. Section

6 of Schedule 10 sets out modifications that are needed to section 146 of the DPA 2018 in order for it to be applied to the PEC Regulations.

631. Clause 90 (4) adds further sub-paragraphs to the end of regulation 5C, which is concerned with the penalties that can be imposed on service providers for failing to report security breaches. New sub-paragraphs 13, 14 and 16 provide the Secretary of State with a power to amend the amount of the fixed monetary penalty that can be imposed (which is currently £1,000 or £800 if paid within 21 days of receipt of the notice of intent). Any changes must be made via regulations which are laid in Parliament and subject to the affirmative resolution procedure. New sub-paragraph 15 provides that, before making regulations under regulation 5C(13), the Secretary of State must consult the Commissioner and "such other persons as the Secretary of State considers appropriate".

632. Clause 90 (5) replaces regulation 31 of the PEC Regulations, which currently applies the Information Commissioner's enforcement powers in the Data Protection Act 1998 to the PEC Regulations. The new regulation 31 will

instead apply certain enforcement powers in Parts 5 to 7 of the DPA 2018 to the PEC Regulations, subject to the modifications in Schedule 10.

633. Clause 90 (6) and (7) remove regulations 31A and 31B, which currently allow the Commissioner to impose “third party information notices” on communications providers to gather information held on electronic communications networks, or by electronic communications services, for investigating compliance with the regulations; and set out rights of appeal against the imposition of a notice. These provisions are no longer needed because the more modern powers in section 142 of the DPA 2018 (Information notices) and associated appeal rights will now be applied to the PEC Regulations. Under these new provisions, the Commissioner will be able to serve a written notice on any person or a communications provider, requesting information or documents to help determine whether the person has or is complying with the PEC Regulations.

634. Under clause 90 (8), the current Schedule 1 to the PEC Regulations, which sets out modifications to the enforcement regime in the

Data Protection Act 1998 for the purposes of their application to the PEC Regulations, is repealed. It is replaced by a new Schedule 10 which sets out modifications to the enforcement regime in the DPA 2018, so that it can be applied to the PEC Regulations.

635. Clause 90 (9) makes some consequential amendments to paragraph 58(1) of Schedule 20 to the DPA 2018 to reflect the changes that have been made to regulations 2, 31 and 31B by these clauses.

Clause 91: Codes of conduct

636. Clause 91 inserts new regulations 32A, 32B and 32C into the PEC Regulations.

637. Under regulation 32A the Information Commissioner must encourage representative bodies to draw up PEC Regulations codes of conduct. Codes of conduct are voluntary accountability tools, enabling sectors to identify key compliance challenges in their sector with the approval of the Information Commissioner that the code, and its monitoring, is appropriate. They are written by an

organisation or association representing a sector in a way that the sector understands.

638. New regulations 32A(1) and (2) require the Information Commissioner to encourage the production of codes of conduct which take account of specific features of different sectors.

639. New regulation 32A(3) sets out an illustrative list of the matters that a code of conduct may make provisions regarding.

640. New regulations 32A(4) and (5) set out the requirements for the Information Commissioner's approval of a code of conduct. Namely, following receipt of a draft code the Commissioner will provide an opinion to the representative body on whether the code correctly reflects the requirements of the relevant PEC Regulations. Codes approved by the Commissioner are to be registered and published.

641. Codes of conduct require a monitoring method, and for private or non-public authorities, a monitoring body to deliver them. New regulation 32A(6) states that the Information Commissioner may only approve codes if they meet these requirements.

642. New regulation 32A(7) sets out how amendments to an approved code will be managed. This provision specifically applies paragraphs (4)-(6) to an amended code

643. New regulation 32A(8) provides for a code of conduct under paragraph (1) to be contained in the same document as a code of conduct described in Article 40 of the UK GDPR and makes it clear that a provision in the code of conduct can address requirements under both the PEC Regulations and the UK GDPR. This will enable the Information Commissionerto give an opinion on whether the code complies with the UK GDPR and relevant PEC Regulations or just relevant PEC Regulations.

644. New regulation 32A(9) sets out the meaning of terms used in the regulation.

645. New regulation 32B permits the Commissioner to accredit a body where the monitoring body meets certain conditions. They include, for example, that the monitoring body has established relevant procedures and structures to handle complaints about infringements of the code, and that it has demonstrated its independence and does not

have a conflict of interest.New regulation 32B(1) permits the Commissioner to accredit a body for the purpose of monitoring a code described under regulation 32A(1). The role of the monitoring body will be to monitor whether an organisation, other than a public body, complies with the code.

646. New regulation 32B(2) sets out the criteria that an organisation must meet to be accredited by the Commissioner as a monitoring body for a code.

647. New regulation 32B(3) requires the Commissioner to publish guidance about how they propose to take decisions about accreditation under this regulation.

648. New regulation 32B(4) requires the monitoring body to take appropriate action where it identifies that an infringement of the code has occurred. If the action taken consists of suspending or excluding a person from the code then the monitoring body is required to inform the Commissioner under new regulation 32B(5) and to provide reasons for why they have taken that action.

649. New regulation 32B(6) requires the Commissioner to revoke a monitoring body's

accreditation if they consider that the body no longer meets the requirements for accreditation, or has failed to take action when the code has been infringed, or has failed to inform the Commissioner when a person has been suspended or excluded from the code.

650. New regulation 32B(7) states that in this regulation the term “public body” has the same meaning as in regulation 32A.

651. New regulation 32(C) sets out that adherence to a code of conduct approved under regulation 32A may be used by a person as a means of demonstrating compliance with the relevant requirements of the PEC Regulations covered by that code.

652. Clause 91(3) amends regulation 33 of the PEC Regulations. The amendment requires Ofcom to comply with any reasonable requests made by the Commissioner in connection with their functions under regulation 32A and regulation 32B.

653. Clause 91(4) amends new Schedule 1 to the PEC Regulation which is inserted by Schedule 10 to this Bill. The amendment adds regulations 32B(4) and 32B(5) to the list of provisions for which a penalty notice may

impose the higher maximum penalty in the event of an infringement.

Clause 92: Pre-commencement consultation

654. Clause 92 makes it clear how consultation requirements under clauses 83 to 90 may be satisfied.

Trust services

Clause 93: The eIDAS Regulation

655. The term “the eIDAS Regulation” in the clauses below refers to Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. The eIDAS Regulation was retained by the European Union (Withdrawal) Act 2018, and amended by The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 S.I. 2019/89.

656. The eIDAS Regulation sets out the legal framework and specifications for trust service products and services in the UK. This system supports the validation of electronic transactions. ‘Trust services’ include services

specifically relating to electronic signatures, electronic seals, timestamps, electronic delivery services, and website authentication. The eIDAS Regulation requires that such trust services meet certain criteria - standards and technical specifications - to allow for interoperability across the UK economy.

Clause 94: Recognition of EU conformity assessment bodies

657. Clause 94 adds new Article 24B to the eIDAS Regulation. This Article allows for the recognition of conformity assessment reports that have been issued by an EU conformity assessment bodies accredited by the national accreditation body of an EU member state, and provides that these reports can be used to grant a trust service provider qualified status under Article 21 of the eIDAS Regulation, and also for the purposes of regular auditing requirements under Article 20(1).

Clause 95: Removal of recognition of EU standards etc

658. Clause 95 sets out that the Secretary of State, by regulations, can amend or revoke Article 24A of the eIDAS Regulation in the

future, should the continued unilateral recognition of EU qualified trust services no longer be appropriate. This power will also allow for the Secretary of State to revoke and amend other provisions of the eIDAS Regulation and associated Implementing Decision (EU) 2015/1506 (which are contingent upon the current recognition of EU qualified trust services and products) including a power to revoke new Article 24B.

Clause 96: Recognition of overseas trust products

659. Clause 96 inserts new Article 45A into the eIDAS Regulation. Article 45A provides the Secretary of State with the power to make regulations to recognise and give legal effect to trust service products provided by trust service providers established outside the UK. The legal effect of overseas trust service products which are specified within regulations, will be equivalent to the legal effect of qualified trust service products provided by a qualified trust service provider established in the UK.

660. There are two conditions which apply when making regulations under Article 45A: the Secretary of State must be satisfied that

the reliability of an overseas trust service product is at least equivalent to the reliability of its qualified counterpart under the eIDAS Regulation; and he must have regard to (among other things) the relevant overseas law concerning the type of trust service product to be recognised.

661. Clause 96 also inserts new Article 45B into the eIDAS Regulation. Existing Articles 27 and 37 of the eIDAS Regulation provide that where public sector bodies require an advanced signature or seal for the use of an online public service, they must recognise electronic signatures and seals which meet advanced standards and additional technical requirements under Commission Implementing Decision 2015/1506. Likewise, where public sector bodies require an advanced signature or seal based on a qualified certificate, they must accept a qualified signature or seal which complies with Commission Implementing Decision 2015/1506. New Article 45B provides the Secretary of State with the power by regulations to recognise, for the use of online public services, specified electronic seals and signatures provided by trust service providers established outside the UK, as equivalent to

electronic seals and signatures under Articles 27(1), 27(2), 37(1) and 37(2) of the eIDAS Regulation which comply with Implementing Decision 2015/1506.

662. The Secretary of State must be satisfied that the reliability of a certain overseas electronic signature or seal is at least equivalent to the reliability of their respective counterpart under the eIDAS Regulation, and must have regard to (among other things) the relevant overseas law concerning the type of electronic signature or seal to be recognised.

663. New Article 45C provides that regulations made under Articles 45A and 45B are able to include conditions which specified overseas trust service products must meet in order to be recognised. Such conditions may include meeting specific requirements within overseas law, or meeting specific technical or regulatory standards.

664. New Article 45C also provides that the Secretary of State must consult the Commissioner as supervisory body for trust services before making regulations under new Articles 45A and 45B.

Clause 97: Co-operation between supervisory

authority and overseas authorities

665. Clause 97 amends Article 18(1) of the eIDAS Regulation to allow the Secretary of State by regulations to designate certain overseas regulators or supervisory bodies, with which the Commissioner as supervisory body for trust services within the UK, may give information, assistance to, or otherwise cooperate with in the interests of effective regulation or supervision trust services. This will replace the ability of the Commissioner to share information and cooperate with any public authority within the EU specifically. New Article 18(4) provides that the Secretary of State must consult the Commissioner, before making regulations under this Article.

666. The amendment made to Article 18(2) is not intended to change the substantive effect of that paragraph. The words in brackets are intended to clarify the relationship between the restrictions in the data protection legislation and the power under new Article 18(1), making clear that this power is to be taken into account when applying the data protection restrictions.

Sharing of information

Clause 98: Disclosure of information to improve public service delivery to undertakings

667. Section 35 of the DEA 2017 provides a legal gateway to enable specified public authorities to share information to improve the delivery of public services to individuals and households. This provision amends section 35 to also enable the sharing of information to improve the delivery of public services to businesses.

668. Section 35 of the DEA 2017 allows only public authorities that are listed in Schedule 4 of the Act to share information for tightly constrained objectives which benefit individuals or households. In addition to being listed in Schedule 4, each public authority must also be authorised by regulations to use the power to share information under each different objective. These same constraints will apply to objectives which have the purpose of improving the delivery of public services to businesses.

669. Under section 35, objectives must be set out in regulations, must be for the

improvement or targeting of the provision of a public service or the provision of a benefit (financial or otherwise) and must also support the delivery of a specified public authority's functions. This includes the administration, monitoring or enforcement of the delivery of the function. These conditions will apply to objectives which have the purpose of improving the delivery of public services to businesses in the same way they apply to objectives relating to individuals and households.

670. Section 35 of the DEA 2017 includes a further requirement that the sharing of information to improve public service delivery to individuals or households must have as its purpose the improvement of the well-being of individuals or households. This provision will require that where information is being shared for the benefit of businesses, objectives have as their purpose the assisting of undertakings in connection with any trade, business or charitable purpose.

671. The provision uses the term "undertakings" for businesses, the definition of which includes any business, whether or not run for profit, along with any organisation established for

charitable purposes. Because the definition of "charitable purposes" is drawn from different Acts in England and Wales, Scotland and Northern Ireland the provision uses the definition from section 2 of the Charities Act 2011 to ensure that a uniform definition is being applied throughout the UK.

Clause 99: Implementation of law enforcement information-sharing agreements

672. Clause 99 provides the appropriate national authority with the power to make regulations to implement the technical and, where appropriate operational detail, of any such international agreements. New international law enforcement information-sharing agreements are subject to usual treaty ratification procedures.

Clause 100: Meaning of "appropriate national authority"

673. This clause defines the "appropriate national authority" by which regulations may be made under Section 99 of this Act as the Secretary of State or, where a provision falls within devolved competence, Scottish Ministers or Welsh Ministers, as stipulated in

subsections (2) to (3).

674. Restrictions in Schedule 7B to the Government of Wales Act 2006 prevent the Senedd from removing, without the consent of the appropriate UK Government Minister, any function of a Minister of the Crown, that relates to a qualified devolved function in that Act. Subsection (5) disapplies the relevant restriction in Schedule 7B of the Government of Wales Act 2006, in respect of the concurrent powers provided in clause 99 of this Act, by adding the Data Protection and Digital Information Act 2023, to the lists of enactments in paragraph 11(6)(b) of Schedule 7B of the Government of Wales Act 2006, to which the general restriction referenced above will not apply.. This allows the Senedd to alter the concurrent arrangements in future without needing the UK Government's consent.

Registers of births and deaths

Clause 101: Form in which registers of births and deaths are to be kept

675. Clause 101 amends the Births and Deaths Registration Act 1953 (the BDRA). Subsection (2) of clause 101 substitutes section 25 of the BDRA (provision of registers, etc, by Registrar General) with a new section 25 (form in which registers are to be kept, etc).

676. Subsection (1) allows the Registrar General to determine how registers of live-births, still-births and deaths are to be kept. This will allow the duplication of processes to be removed, such as the requirement for paper registers to be held and stored securely in each registration district whilst at the same time being registered in an electronic register. Instead, all births, still-births and deaths may be registered in an electronic register and stored electronically without the need for paper registers to be kept securely in a safe.

677. Subsection (2) allows the Registrar General to require that registrars keep information in a form that allows the Registrar General and the superintendent registrar to

have immediate access to all birth and death entries as soon as the details have been entered in the electronic register by the registrar. Subsection (2)(b) allows only the Registrar General to have immediate access to entries of still-births which have been registered, by the registrar, in the electronic register.

678. Subsection (3) provides that where a register is kept in such form as mentioned in subsection (2), e.g. electronic form, any information held in that register which has been made available to the Registrar General and the superintendent registrar is deemed to be 'held' by that person, as well as the registrar, when carrying out that person's functions.

679. Subsection (4) places responsibility on the Registrar General to provide and maintain anything that is required for the purpose of creating or maintaining the registers referred to in subsection (1), for example, providing registrars with the system needed to register births and deaths.

680. Subsection (5) places a responsibility on the Registrar General to provide the forms that

are required in order to produce certified copies of entries in the registers – for example, a birth or death certificate.

681. Clause 101 (3)(a) and (b) omit sections 26 and 27 of the BDRA which set out the requirements for quarterly returns made by a registrar and superintendent registrar. With the introduction of an electronic register there will no longer be a requirement for the system of quarterly returns as all birth and death entries will be held in a single electronic register and the Registrar General and superintendent registrar will have immediate access to all birth and death entries.

682. Clause 101(3)(c) omits section 28 (custody of registers, etc) which sets out how paper birth and death registers need to be stored by registrars, superintendent registrars and the Registrar General. With the introduction of an electronic register this provision will no longer be required. The requirements for the retention and storage of existing paper registers are covered in clause 104.

Clause 102: Provision of equipment and facilities by local authorities

683. Clause 102 inserts a new section 11A (Provision of equipment and facilities by local authorities) in the Registration Service Act 1953. Subsections (1) and (2) set out how the council of every non-metropolitan county and metropolitan district (subject to the provisions of their local scheme arrangements) must provide and maintain equipment or facilities that the Registrar General considers necessary for a superintendent registrar or registrar to carry out their functions. This requirement applies across each register office or sub-district of a registrar.

Clause 103: Requirements to sign register

684. Clause 103 makes further amendments to the BDRA.

685. Subsection (2) inserts a new section 38B (Requirements to sign register) which empowers the Minister to make regulations that provide for the following, in relation to registers of births or deaths that are not kept in paper form:

- that a duty to sign a birth or death register at the time of registration is to have effect as a duty to comply with specified requirements;
- that a person who complies with specified requirements is to be treated as having signed the register at that time and to have done so in the presence of a registrar, and the entry in the register will be treated as having been signed by the person;

686. Under new section 38B(2) the provision that may be made by the regulations includes:

- provision requiring a person to sign something other than the register;
- provision requiring the person to provide evidence of identity, specified in regulations, when registering a birth or death.

687. New section 38B(3) clarifies that in this section "specified" means specified in regulations under this section.

688. Subsection (3) inserts a new subsection (6) in section 39A of the BDRA (regulations made by the Minister: further provisions) that states regulations made by the Minister under

section 38B may not be made unless they are laid before and approved by both Houses of Parliament (affirmative procedure).

Clause 104: Treatment of existing registers and records

689. Clause 104 (1) specifies that the repeal of section 28 of the BDRA by clause 97 (3)(c) does not affect the following:

- the requirement under section 28(2) of the BDRA for every superintendent registrar to continue to keep any records in their office of any registers of live-births or deaths which are in their custody immediately before the repeal comes into force;
- the requirement under section 28(4) of the BDRA for the Registrar General to continue to keep any certified copies (quarterly returns) which are in the possession of the Registrar General and that such records need to be retained as per existing procedures. The Registrar General is also required to keep any registers of still-births that were forwarded to the Registrar General before the coming into force of the repeal and such records

need to be kept as per existing procedures.

690. Subsection (2) places a requirement on registrars to send any unfilled paper register of births or deaths, which are in their possession before this clause comes into force, to the superintendent registrar for them to be kept by the superintendent registrar.

691. Subsection (3) places a requirement on registrars to send any unfilled paper register of still-births, which are in their possession before this clause comes into force, to the Registrar General for them to be kept by the Registrar General at the General Register Office.

692. Subsection (4) allows the Registrar General to dispose of certified copies (quarterly returns) of still-birth entries in any register of still-births received under section 28(3) of the BDRA or under subsection (3) of clause 94 above. The Registrar General may also dispose of any information contained in those entries and held by the Registrar General in electronic form by virtue of section 27 of the BDRA.

693. Subsection (5) specifies how copies of registers of births and deaths which have been

held in any form other than hardcopy form (such as electronically) during the period outlined in subsection (6) are to be treated:

- subsection (5)(a) provides that those copies of birth and death registers are to be treated as the register for the sub-district on and after the day clause 1 comes into force;
- subsection (5)(b) provides that the register is to be treated for the purposes of section 25(3) of the BDRA as having been kept in the form in which the copy was kept;
- subsection (5)(c) provides that any entry in the register signed by a person before clause 1 comes into force is to be treated as having been signed by the person for the purposes of the BDRA;
- subsection (5)(d) allows the Registrar General to dispose of any certified copies received under section 27 of the BDRA and any information contained in those entries where they are also kept in electronic form.

694. Subsection (6) outlines the period referred to in subsection (5) as (a) beginning on 1 July

2009, and (b) ending immediately before the day clause 97 comes into force.

Clause 105: Minor and consequential amendments

695. Clause 105 brings Schedule 11 into effect.

Information standards for health and social care

Clause 106: Information standards for health and adult social care in England

696. Clause 106 makes provision about information standards for health and adult social care in England and information technology. It gives effect to Schedule 12 which amends Part 9 of the Health and Social Care Act 2012.

Part 5: Regulation and Oversight

Information Commission

Clause 107: The Information Commission

697. Together, clauses 107, 108, 109, 110 and Schedule 13 establish a body corporate, the Information Commission, to replace the existing regulator, the Information Commissioner, which is currently structured as a corporation sole. The office of the Information Commissioner is abolished, and provision is made for the transfer of functions from the Information Commissioner to the new body, and for the current Information Commissioner to transition to the role of chair of the Information Commission.

698. Clause 107 inserts a new section 114A into the DPA 2018, which establishes the Information Commission. Schedule 13 inserts a new Schedule 12A into the DPA 2018, which makes further provision about the new body.

Clause 108: Abolition of the office of Information Commissioner

699. Clause 108 makes provision for the abolition of the office of Information

Commissioner.

700. Subsection (1) abolishes the office of Information Commissioner.

701. Subsections (2)-(7) make amendments to the DPA 2018.

Clause 109: Transfer of functions to the Information Commission

702. Clause 109 makes provision for the transfer of functions from the Information Commissioner to the Information Commission.

703. Subsection (1) transfers the functions of the office of Information Commissioner to the new body corporate, that is the Information Commission.

704. Subsection (2) makes provision for references to the Information Commissioner in enactments or other documents (whenever passed or made) to be treated as references to the Information Commission so far as appropriate in consequence of the transfer of functions under subsection (1).

705. Subsection (3) defines enactments on which the provision at subsection (2) operates.

Clause 110: Transfer of property etc to the Information Commission

706. Subsection (1) provides that the Secretary of State may make a scheme for the transfer of property, rights and liabilities from the Information Commissioner to the Information Commission.

707. Subsection (2) sets out the things that may be transferred under any such scheme.

708. Subsection (3) sets out the nature and scope of the transfer scheme.

709. Subsection (4) provides for modifications to be made to the transfer scheme.

710. Subsection (5) explains that references to rights and liabilities in subsection (3) include rights and liabilities relating to a contract of employment.

Oversight of biometric data

Clause 111: Oversight of retention and use of biometric material

711. Section 20 of the Protection of Freedoms Act 2012 (POFA) brought in a requirement for the Secretary of State to appoint a

Commissioner for the Retention and Use of Biometric Material for England and Wales (the Biometrics Commissioner). The Biometrics Commissioner is responsible for two casework functions: reviewing decisions by chief officers of police to approve the retention of biometrics beyond ordinary statutory limits on national security grounds[8], and reviewing applications to retain biometrics on other public safety grounds, where the individual has not been convicted[9]. The Biometrics Commissioner also reviews police retention and use of DNA and fingerprints and reports annually to the Home Secretary on compliance with the relevant legislation set out in POFA. These reports are laid in parliament. These duties are set out in sections 20 and 21 of POFA.

712. Clause 111 amends section 20 of POFA to abolish the office of the Biometrics Commissioner and transfers the casework functions set out above to the Investigatory

[8] National Security Determinations can be made or renewed by chief officers of police under various powers, currently set out in s20(2)(a) of POFA. The chief officer making or renewing the National Security Determination must have reasonable grounds to believe that the retention is necessary for the purpose of national security and proportionate to the aim sought to be achieved.

[9] This process is set out in s63G of the Police and Criminal Evidence Act 1984 (PACE). Applications may be submitted under s63G of PACE where a chief officer of police considers that, where an individual has been arrested, but not charged with, a qualifying offence, the individual's DNA and fingerprints should be retained, beyond ordinary statutory limits, for wider public safety reasons. The permitted reasons are set out under s63G(2) and (3).

Powers Commissioner, appointed under the Investigatory Powers Act 2016 (IPA). This will reduce duplication and simplify oversight of the police use of biometrics. The Information Commissioner will continue to provide independent oversight of the use of biometrics by all bodies, including the police.

713. Subsection (4)(c) transfers oversight of the National Security Determinations regime to the Investigatory Powers Commissioner, including the power to order the destruction of fingerprints and DNA profiles where he or she is not satisfied that retention would be necessary and proportionate for national security. This subsection also transfers the functions under section 63F(5)(c) and 63G of the Police and Criminal Evidence Act 1984 (PACE) to the Investigatory Powers Commissioner. These functions relate to determining (in response to applications by the police) whether the fingerprints and DNA profiles of persons arrested for, but not charged with, a qualifying offence[10] may be

[10] Qualifying offences are more serious offences such as murder, manslaughter, rape, wounding, grievous bodily harm, assault occasioning actual bodily harm, robbery and burglary. The full list of qualifying offences is set out in section 65A of PACE.

retained pursuant to the provisions in section 63G of PACE.

714. Subsection (4)(d) removes the function to review the retention and use, by the police and others, of fingerprints and DNA profiles not subject to a National Security Determination, whether this biometric material has been taken and retained under PACE, the Terrorism Act 2000, the Counter-Terrorism Act 2008, or the Terrorism Prevention and Investigation Measures Act 2011. This removes duplication in oversight, as the Information Commissioner has a duty to keep under review the use and retention of personal data by all controllers, including the police.

715. Subsection (4)(g) ensures that the Investigatory Powers Commissioner is subject to similar duties in the exercise of the above functions as he or she is in carrying out other existing duties under the Investigatory Powers Act 2018 with the exception of the duties in relation to error reporting. In the case of applications under section 63G of PACE, an individual has the right to make representations about the retention of these so there is an opportunity to raise concerns at this point. Subsection (4)(g) also clarifies that the

Investigatory Powers Commissioner must include information on the use of National Security Determinations and applications under section 63G of PACE in his or her annual report.

716. In line with abolishing the office of Biometrics Commissioner, subsection (5) repeals the corresponding requirement for the Biometrics Commissioner to publish an annual report. Subsection (4)(g) above provides that there will be continued reporting to parliament on the use of National Security Determinations and applications under section 63G of PACE by the Investigatory Powers Commissioner.

717. Subsection 6) makes minor changes to section 22 of POFA in relation to guidance on making National Security Determinations. Subsection (6)(b) allows the Secretary of State to lay updated guidance in parliament as a final version without needing to specify the changes that have been made. Updated guidance will still require approval by a resolution of each House of Parliament to come into force.

718. Subsections (7) – (10) update the relevant provisions within PACE to reflect the removal

of the Biometrics Commissioner and transfer of functions to the Investigatory Powers Commissioner (as set out in the subsections above).

Clause 112: Removal of provision for regulation of CCTV etc

719. Chapter 1 of Part 2 of POFA (Regulation of CCTV and other surveillance camera technology) introduced a requirement for the Secretary of State to prepare a code of practice containing guidance on surveillance camera systems (the Surveillance Camera Code), including Closed Circuit Television (CCTV) and Automatic Number Plate Recognition (ANPR) systems. Authorities listed under section 33(5) must have regard to this code, essentially local authorities, police and crime commissioners and chief constables. Other organisations can also voluntarily adhere to the Code. Chapter 1 introduced a requirement for the Secretary of State to appoint a Surveillance Camera Commissioner to encourage, and report on, compliance with the Code.

720. Clause 112 subsection (1) abolishes the office of Surveillance Camera Commissioner.

Subsection (2) repeals Chapter 1 of Part 2 of POFA, repealing the requirement for a Surveillance Camera Code and related provisions. This removes duplication in oversight of overt surveillance (for example CCTV systems) used by the police and local authorities. The Information Commissioner already has oversight of the use of personal data under the Data Protection Act 2018, including data captured via surveillance camera systems, by all controllers, including the police and local authorities. The Information Commissioner's Office has also published guidance on the use of such systems. This means that the Information Commissioner will continue to provide independent oversight and regulation of this area, without duplication by the Surveillance Camera Code and Commissioner, making it easier for the police, local authorities and the public to understand and comply with any requirements.

Clause 113: Oversight of biometrics databases

721. Section 24 of POFA inserted section 63AB into PACE. This introduced a statutory board to oversee the operation of the National DNA

Database - the National DNA Database Strategy Board. This requirement is being delivered through the Forensic Information Databases Strategy Board (FIND-SB).

722. Clause 113 amends section 63AB of PACE by increasing the scope of the statutory board to also provide oversight of the national fingerprint database (referred to as IDENT1). This brings the legislation up to date with the latest published governance rules for the FIND-SB, which added oversight of the national fingerprint database into the board's terms of reference. Clause 1135 also updates the name of the statutory board so it is consistent with the working title.

723. Clause 113 also introduces a new power for the Secretary of State to change the databases the FIND-SB oversees by adding or removing a biometric database used for policing purposes. The regulations to enable this will be made under the affirmative procedure. This power is intended to enable flexibility in the board's remit given the pace of technological change in this area and the need for clear and consistent oversight. To support policing to meet the requirements of the DPA and PACE, the FIND-SB will produce codes of

practice on the destruction of biometric material and erasure of this data from a database.

Part 6: Final Provision

Clause 114: Power to make consequential amendments

724. This clause gives the Secretary of State a regulation-making power to make amendments to other legislation which are consequential to provisions in this Bill, as well as to this Bill itself where such amendments are consequential to the abolition of the Information Commissioner and his replacement by the new Information Commission. Any regulations proposed under this power which amend or repeal primary legislation are subject to the affirmative procedure. Any other regulations are subject to the negative procedure.

Clause 115: Regulations

725. This clause makes provision concerning the form and procedure for making regulations under the powers in the Bill.

Clause 116: Interpretation

726. This clause is self-explanatory in explaining the meaning of references to “the 2018 Act” and “the UK GDPR” in the Bill.

Clause 117: Financial provision

727. This clause authorises expenditure arising from the Bill, further information about which can be found under “Parliamentary approval for financial costs or for charges imposed” below.

Clause 118: Extent

728. Detailed analysis of the extent of the Bill can be found at Annex A. Otherwise, this clause is self-explanatory.

Clause 119: Commencement

729. This clause gives the Secretary of State a regulation-making power to bring the Bill’s provisions into force. Some provisions, listed in subsection (2), come into force on the data of Royal Assent. Other provisions, listed in subsection (3), come into force two months after Royal Assent. Further information about when provisions will be commenced can be found under “Commencement” below.

Clause 120: Transitional provision

730. This clause gives the Secretary of State a regulation-making power to make transitional, transitory or saving provisions that may be needed in connection with any of the Bill's provisions coming into force, including changes to such provisions in Schedule 21 to the DPA 2018 (Further transitional provision etc.) and Part 2 of Schedule 7 to this Bill (Transfers of personal data to third countries etc: consequential and transitional provision).

Clause 121: Short title

731. This clause is self-explanatory.

Schedules

SCHEDULE 1: LAWFULNESS OF PROCESSING: RECOGNISED LEGITIMATE INTERESTS

732. Schedule 1 inserts a new Annex 1 into the UK GDPR setting out the conditions for constituting a recognised legitimate interest for

the purposes of new Article 6(1)(ea) UK GDPR (as inserted by clause 5). The amendment made to Article 6(1) by clause 5(2)(c) ensures that public authorities cannot rely on these conditions when processing in the performance of their tasks.

733. Paragraph 1 provides a condition for processing where it is necessary for the purposes of making a disclosure to a controller who needs to process that data for its task in the public interest or exercise of official authority pursuant to Article 6(1)(e), in circumstances where the controller has made a request for the personal data. Paragraph 1 would enable a controller to respond to such a request where it considered that the provision of the personal data was necessary. The amendment made to Article 6(1)(e) by clause 5(a) ensures that paragraph 1 provides the only circumstance in which a controller can rely on another controller's tasks in the public interest.

734. Paragraph 2 provides a condition for processing where it is necessary for the purposes of safeguarding national security, protecting public security or for defence purposes.

735. Paragraphs 3 and 4 provide a condition for processing where it is necessary for responding to an emergency as defined in the Civil Contingencies Act 2004. This condition will be relevant where there is an event or situation which threatens serious damage to human welfare or the environment in the whole, a part or a region of the UK, or where there is war or terrorism which threatens serious damage to the security of the UK. The Civil Contingencies Act 2004 lists a series of events that further define the meaning of these events or situations, including loss of human life, human illness or injury, homelessness etc.

736. Paragraph 5 provides a condition for processing where it is necessary for the purposes of detecting, investigating or preventing crime or apprehending or prosecuting offenders. The reference to 'crime' would also cover economic crimes such as fraud, money-laundering, terrorist financing etc.

737. Paragraph 6 provides a condition for processing where it is necessary for the purposes of safeguarding a child or vulnerable adult who is over 18 and considered to be at

risk. Paragraphs 7 and 8 elaborate on what these concepts mean.

738. Paragraph 9 provides a condition for processing where it is necessary for democratic engagement purposes and relates to a data subject who is aged 14 years or over. This reflects the variations in voting age across the nation, where in some parts of the UK, such as Scotland, a person can register to vote at the age of 14 as an attainer. For these purposes, 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.

739. Paragraph 10 clarifies when processing is carried out for democratic engagement purposes. This will apply to processing by elected representatives (or persons acting under their authority) necessary to carry out their functions or for the purposes of their

democratic engagement activities. It will also apply to political parties or persons registered under s 23 of the Political Parties, Elections and Referendums Act 2000 carrying out processing necessary for their democratic engagement activities, for the purposes of assisting elected representatives with their functions or democratic engagement activities and for the purposes of assisting with a candidate's campaign for an election. Democratic engagement also includes processing necessary for the purposes of a candidate's campaign for an election, and processing necessary for the campaigning of permitted participants in a referendum and processing by accredited recall petitioners necessary for campaigning in connection with a recall petition. Anyone carrying out necessary processing for these purposes and acting under the authority of these people are also covered.

740. Paragraphs 11-14 sets out various definitions relevant to processing for democratic engagement purposes.

SCHEDULE 2: PURPOSE LIMITATION: PROCESSING TO BE TREATED AS COMPATIBLE WITH ORIGINAL PURPOSE

741. Schedule 2 inserts a new Annex 2 into the UK GDPR, which sets out the conditions referred to in new Article 8A(3)(d). If further processing meets any of these conditions, the processing is to be treated as compatible with the original purpose. The conditions do not require that the processing be otherwise authorised in legislation or through a rule of law. Where the original lawful basis for processing was consent (Article 6(1)(a) UK GDPR), use of the conditions in the Annex is subject to consideration by the controller of whether it would be reasonable to seek the data subject's consent (Article 8A(4)(b)).

742. Paragraph 1 treats further processing as compatible where it is necessary for the purposes of making a disclosure to a controller ("A") who needs to process that data for its task in the public interest or exercise of official authority, pursuant to Article 6(1)(e), in circumstances where controller A has made a request for the personal data. Paragraph 1 would enable a controller ("B") to respond to

such a request from controller A without having to consider whether the new purpose is compatible with the purpose at the point of data collection. Controller B must not be a public authority carrying out processing in performance of its tasks..

743. Paragraph 2 treats further processing as compatible where it is necessary for the purposes of protecting public security. National security and defence purposes are not included in Annex 2 as there is already an exemption from the purpose limitation principle in section 26 of the DPA 2018.

744. Paragraphs 3 and 4 treat further processing as compatible where it is necessary for responding to an emergency as defined in the Civil Contingencies Act 2004. This condition will be relevant where there is an event or situation which threatens serious damage to human welfare or the environment in the whole, a part or a region of the UK, or war or terrorism which threatens serious damage to the security of the UK. The Civil Contingencies Act 2004 lists a series of events that further define the meaning of these events or situations, including loss of human life, human illness or injury, homelessness etc.

745. Paragraph 5 treats further processing as compatible where it is necessary for the purposes of detecting, investigating or preventing crime or apprehending or prosecuting offenders. The reference to ‘crime’ would also cover economic crimes such as fraud, money-laundering, terrorist financing etc.

746. Paragraph 6 treats further processing as compatible where it is necessary for the purposes of protecting the vital interests of the data subject or another individual.

747. Paragraph 7 treats further processing as compatible where the processing is necessary for the purposes of safeguarding a child or adult who is over 18 and considered to be at risk in ways defined in paragraph 9.

748. Paragraph 10 treats further processing as compatible where processing is carried out for the purpose of assessment or collection of a tax or duty or an imposition of a similar nature.

749. Paragraph 11 treats further processing as compatible where processing is necessary for the purposes of complying with an obligation of a controller under an enactment, a rule of law or an order of a court or tribunal.

SCHEDULE 3: AUTOMATED DECISION-MAKING: CONSEQUENTIAL AMENDMENTS

750. Schedule 3 makes consequential amendments to the UK GDPR and the DPA 2018. These amendments are required to ensure consistency as a result of the changes made to the new Article 22A-D in clause 12.

SCHEDULE 4: OBLIGATIONS OF CONTROLLERS AND PROCESSORS: CONSEQUENTIAL AMENDMENTS

751. Schedule 4 makes consequential amendments to the UK GDPR and the DPA 2018. These amendments are required as a result of the changes made to words and associated new definitions in clauses 14, 15, 17, and 18.

SCHEDULE 5: TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES ETC: General processing

752. Chapter 5 of the UK GDPR sets out the conditions under which personal data can be transferred to a country outside of the UK or an international organisation (as defined in Article 4 of UK GDPR). Schedule 5 makes various

amendments to Chapter 5 of the UK GDPR, to reform the UK's regime for international transfers, as explained below.

753. Schedule 5 (2)(1) omits Article 44 and replaces it with a new Article 44A.

754. Article 44A(1) and (2) set out the three legal bases under which personal data can be lawfully transferred overseas. The first basis is where the Secretary of State has made regulations allowing the free flow of personal data to another country (see Article 45A-C). The second basis is where appropriate safeguards for the personal data are provided under Article 46. For example, organisations may put contractual clauses in place with recipient organisations overseas to ensure the personal data is treated safely and securely. The third basis is where a transfer can be made based on a derogation under Article 49.

755. Schedule 5 (3) to (5) omit Article 45. Article 45 currently provides that transfers of personal data to another country could take place where the Secretary of State has made regulations finding that the country in question provided an adequate level of protection. The free flow of personal data is then allowed to this country.

756. In place of Article 45 and sections 17A and 17B of the DPA 2018, which are omitted by Schedule 7, paragraphs 11 and 12, Schedule 5 (4) and (5) insert new Articles 45A, Article 45B and Article 45C. Previously the provisions relating to adequacy regulations were found partly in the DPA 2018, and partly in Chapter 5 of the UK GDPR. The effect of the provisions in Schedule 5 and Schedule 7 will be that all provisions relating to the approval of transfers to other countries or international organisations will now be contained in Chapter 5 of the UK GDPR.

Approving transfers of personal data

757. Article 45A(1) provides a power for the Secretary of State to make regulations approving transfers of personal data to a third country or international organisation, thus allowing the free flow of personal data to that country or international organisation, as with the previous power to make adequacy regulations which was dealt with in section 17A of the DPA 2018 and Article 45 UK GDPR. Where such regulations are in place, UK organisations will not require any further authorisation to make a transfer of personal

data to that country or international organisation, provided the transfer falls within the terms of the regulations. An international organisation could be within the UK or overseas. International organisation is defined in Article 4; examples of international organisations include UN bodies.[11]

758. Article 45A(2) specifies that the Secretary of State may only make regulations approving transfers if the Secretary of State is satisfied that the data protection test is met. The data protection test is set out in Article 45B, which is explained below.

759. Article 45A(3) specifies that the Secretary of State may consider other matters that he or she considers relevant when he or she makes regulations. Other relevant matters may include consideration of the desirability of facilitating transfers of personal data to and from the UK and how they will benefit the UK. While ultimately all countries must meet the same high data protection standards in order to have regulations made approving transfers to them, the wider context of data flows

[11] Article 4 defines an international organisation as: *an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries*

between the UK and another country may be important when deciding whether to make regulations.

760. Article 45A(4) provides flexibility for regulations to be made covering some or all transfers to a country or international organisation. While regulations could be made approving all transfers to a particular country or international organisation, Article 45A(4) provides flexibility for the regulations to be more targeted and only approve certain transfers to that country or international organisation - for example, transfers to a particular sector or geographic area within the country, transfers to certain recipients or by certain UK organisations, transfers of certain types of personal data, or transfers identified in another way.

761. Article 45A(5) provides that regulations under Article 45A are subject to the negative resolution procedure.

The data protection test

762. Article 45B sets out the data protection test which the Secretary of State must consider is met in order to make regulations approving transfers to a country or international

organisation.

763. Article 45B(1) provides that the data protection test is met if the standard of protection for the general processing of personal data in that country or international organisation is not materially lower than the standard of protection under the UK GDPR and relevant parts of the DPA 2018. The test therefore makes clear that:

- the Secretary of State should consider the standard of protection for data subjects within the third country, in a holistic way. This is further clarified in Article 45B(3) which confirms that references to protection in the data protection test are to that protection taken as a whole. This means that the test does not require a point- by-point comparison between the other country's regime and the UK's regime or for the destination country to take the same legal and cultural approach as the UK. Instead, the Secretary of State's assessment will be based on outcomes, such as the overall standard of protection for a data subject;
- the Secretary of State will assess whether

the standard of protection is materially lower than the UK's standard. The test recognises that other countries' data protection regimes will not be identical to the UK's in form and differences may exist given the cultural context of privacy. Therefore, protections in a third country do not need to be identical to those in the UK. Instead, the Secretary of State must exercise his or her discretion, in a holistic and contextual manner, to decide whether or not the overall standard of protection is lower than the UK's standard in a way which is material;

- the standard of protection in the third country or international organisation must not be materially lower than the standard of protection which applies under the UK's regime for the general processing of personal data. The UK's regime for general processing is contained within the UK GDPR and Part 2 and Parts 5-7 of the DPA 2018. It does not include Parts 3 and 4 DPA 2018, which govern processing by law enforcement bodies and the intelligence services respectively.

764. Article 45B(2) sets out a more concise and

streamlined list of matters which the Secretary of State must consider as part of deciding whether the data protection test is met. These include:

- respect for the rule of law and for human rights in the country or the international organisation;
- the existence, and powers, of an enforcement authority. This requires the Secretary of State to consider how such an authority protects UK data subjects in relation to their personal data which has been transferred;
- arrangements for redress for data subjects, whether that redress is judicial or non-judicial: the Secretary of State is required to consider the redress available for data subjects. The provision recognises that redress arrangements will differ by country. For example, redress could be provided by administrative authorities instead of or in addition to judicial redress;
- rules about the transfer of personal data from the country or by the organisation to other countries or international organisations. The Secretary of State must

consider how the country or international organisation ensures that personal data continues to be appropriately protected when it is transferred onwards to another country or international organisation;

- any relevant international obligations to which the country or international organisation is subject. This might include whether they are party to multilateral or regional agreements relevant to data protection or related matters. For example, the European Convention on Human Rights, or the Council of Europe Convention of 28 January 1981 for the Protection of Individuals ("Convention 108");
- the constitution, traditions and culture of the country or organisation. This requires the Secretary of State to consider the constitutional and cultural traditions that may contribute to a country or organisation's approach to data protection, which may differ from those in the UK.
- Article 45B(2) is a non-exhaustive list and the Secretary of State may also need to consider other matters in order to

determine whether the required standard of protection exists. For example, where there are laws and practices in the third country regarding how public authorities access personal data for national security or law enforcement purposes, to the extent that they affect the overall standard of protection, the Secretary of State will take these into account.

765. Article 45B(3) makes further provision about the way in which the data protection test operates, including providing that references to the protection for data subjects mean that protection taken as a whole, and that references to the processing of personal data in the third country mean the processing of personal data transferred to the country or organisation under the UK GDPR (and not, for example, other personal data derived from within that third country).

766. Article 45B(4) clarifies that where the Secretary of State makes regulations which only apply to some transfers to a country or international organisation, the relevant requirements and provisions in Article 45B only refer to the transfers permitted by the regulation, and the reference to rules for

onward transfers includes rules on transfers elsewhere within that country as well as outside of it.

Monitoring

767. Schedule 5 (5) inserts Article 45C into the UK GDPR, replacing section 17B of the DPA 2018 which has been omitted by Schedule 7, paragraph 12.

768. Article 45C(1) requires the Secretary of State to monitor developments in third countries and international organisations that could affect decisions to make regulations approving transfers of personal data under Article 45A, or decisions to amend or revoke such regulations. Ongoing monitoring of countries' relevant laws and practices will enable the Secretary of State to respond to any developments that might affect decisions to make, amend or revoke regulations under Article 45A. Such monitoring might include, for example: engaging in dialogue with country representatives; obtaining information from HMG Embassies or High Commissions; commissioning and/or reviewing third party reports; and engaging with the Commissioner.

769. Article 45C(2) provides that if the Secretary of State becomes aware that the data protection test is no longer met in relation to a country or international organisation to which transfers have been approved, the Secretary of State must either amend or revoke the regulations approving transfers to that country of international organisation. For example, an amendment may limit the types of transfer that are permitted by the regulation. If there is no way of amending the regulation to meet the data protection test the Secretary of State must revoke it. If the regulations are revoked the transfer of personal data to that third country or international organisation may still take place where other appropriate legal bases, as set out in Article 46 and Article 49 apply.

770. Article 45C(3) provides that when regulations are amended or revoked, the Secretary of State must enter into consultations with the third country or international organisation concerned with a view to improving the protection provided to data subjects in relation to their personal data.

771. Article 45C(4) requires the Secretary of State to publish a list of third countries and

international organisations which are for the time being approved by regulations under Article 45A. The Secretary of State is also required to publish a list of the third countries and international organisations which have been, but are no longer, approved by such regulations. The government intends to publish this information on GOV.UK. Article 45C(5) requires the lists published under Article 45C(4) to specify where only certain transfers to that country or international organisation are approved.

Transfers subject to appropriate safeguards

772. Schedule 5 (5) amends Article 46 and 47 of the UK GDPR and introduces new Article 47A.

773. Paragraph 6(1) of Schedule 5 is self-explanatory.

774. Paragraph 6(2) omits existing Article 46(1), which currently provides that, in the absence of adequacy regulations, a controller or processor may transfer personal data to a third country or international organisation only if they provide appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies are available. Existing Articles

46(2) and (3) provide further detail on how appropriate safeguards may be provided.

775. Paragraph 6(3) inserts new Article 46(1A) and provides that a transfer of personal data is made to a third country or international organisation subject to appropriate safeguards only if:

- safeguards (such as the transfer mechanisms described in existing Articles 46(2) or (3) or specified in regulations pursuant to new Article 47A(4)) are provided in connection with the transfer. If the safeguards are provided by an instrument described in existing Article 46(2)(a), the transfer must be consistent with the intended scope of the instrument; and
- where the safeguard is a mechanism described in existing Article 46(2)(b) - (f), (3)(a) - (b) or specified in regulations pursuant to new Article 47A(4), the controller or processor, acting reasonably and proportionately, considers that the data protection test is met in relation to the transfer or type of transfer; or
- where the safeguard is an instrument

described in existing Article 46(2)(a), each UK public body that is a party to the instrument, acting reasonably and proportionately in the circumstances, considers that the data protection test is met in relation to the transfers or types of transfer which is intended to be made in reliance on the instrument.

776. Paragraphs 6(4)(a)(i), (e) and (f) make consequential amendments to existing Article 46(2) to clarify that the word 'safeguards' refers only to the transfer mechanisms listed in existing Article 46(2), the use of which is only appropriate in all the circumstances if the controller, processor or public body that is party to the instrument, acting reasonably and proportionately, considers that the data protection test is met. Paragraph 6(4)(c) makes a clarificatory amendment to confirm that binding corporate rules provide safeguards for the purposes of new Article 46(1A) only if they are approved pursuant to Article 47. Paragraphs 6(4)(a)(ii), (b) and (d) are self-explanatory.

777. Paragraph 6(5)(a) makes a consequential amendment to existing Article 46(3) to clarify that the word 'safeguards' refers only to the

transfer mechanisms listed in existing Article 46(3), the use of which is only appropriate in all the circumstances if the controller or processor, acting reasonably and proportionately, considers that the data protection test is met. Paragraphs 6(5)(b) to (d) are self-explanatory.

778. Paragraph 6(6) introduces the new data protection test in new Article 46(6), which the controller, processor or UK public body that is party to the instrument, acting reasonably and proportionately, must consider is met before a transfer under Article 46 may take place. The data protection test is met if, after the personal data being transferred has reached its destination, the standard of protection provided for the data subject (by the safeguards and other means, where relevant) would not be lower than the standard of protection under the UK GDPR and relevant parts of the DPA 2018 in a way which is material. This includes relevant enforceable data subject rights and effective legal remedies for the data subject in all the circumstances of the transfer. The new test also recognises that safeguards may be applied in different cultural and legal contexts when being used internationally and still

provide appropriate protection for data subjects, and is consistent with the approach taken in the revised Article 45. The test, therefore, does not require a point by point comparison of protections for data subjects, which would not be reasonable or proportionate given the ways in which data protection regimes may differ.

779. Paragraph 6(6) also introduces new Article 46(7), which provides more detail about what it means to act reasonably and proportionately. It clarifies that the actions of a controller, processor or UK public body that is party to an instrument must be reasonable and proportionate in all the circumstances (or likely circumstances) of the transfer (or types of transfer) - this includes considering the nature and volume of the personal data being transferred. This process is distinct to that which the Secretary of State undertakes under new Articles 45A and B. It is tailored for the purposes of controllers or processors (or UK public bodies that are parties to an instrument under existing Article 46(2)(a)), and recognises that the transfer mechanisms in existing Articles 46(2) and (3) or specified in regulations pursuant to new Article 47A(4)

include inherent protections for the rights of data subjects.

780. Finally, paragraph 6(6) introduces new Article 46(8), which:

- clarifies that references to the protection for the data subject are to that protection taken as a whole; and
- introduces the definition of a ‘relevant person’ to distinguish from public bodies as defined in Article 4(10A). A ‘relevant person’ for the purposes of existing Articles 46(2)(a) and 3(b) means a public body or another person (including an international organisation) exercising functions of a public nature.

781. Paragraph 7 is self-explanatory.

Making provision about further safeguards for transfer

782. Schedule 5 (5) inserts Article 47A, which makes further provision about transfers subject to appropriate safeguards.

783. New Articles 47A(1) to (3) restate existing sections 17C(1), (2) and (3) of the DPA 2018, which are omitted by Schedule 7. Previously

the provisions relating to transfers subject to appropriate safeguards were found partly in the DPA 2018 and partly in Chapter 5 of the UK GDPR. The effect of the provisions in Schedule 5 and Schedule 7 will be that all provisions relating to transfers subject to appropriate safeguards will now be contained in Chapter 5 of the UK GDPR.

784. New Article 47A(4) to (7) provides a power for the Secretary of State to make provision, by way of regulations (subject to affirmative procedure), about further safeguards that may be relied on for the purposes of making a transfer under Article 46 (transfer subject to appropriate safeguards). The new power can only be exercised if the Secretary of State considers that the further safeguards are capable of ensuring that the data protection test in new Article 46(6) is met in relation to the transfers of personal data generally or in relation to a type of transfer specified in the regulations.

Derogations for specific situations

785. Schedule 5 (9) makes consequential amendments to Article 49 (derogations for specific situations) which are required as a

result of the changes elsewhere in Chapter 5 of the UK GDPR, which are explained above.

786. Schedule 5 (9) also inserts a new sub-paragraph (4A). This sub-paragraph sets out the provision formerly included in section 18(1) DPA 2018, as part of the restructuring so that all provisions on international transfers are now contained within Chapter 5 of the UK GDPR. It continues the same power for the Secretary of State to specify in regulations, for the purposes of Article 49(1)(d), circumstances in which a transfer of personal data is to be taken as necessary, or not necessary, for important reasons for public interest.

Public interest restrictions

787. Schedule 5 (10) inserts Article 49A which contains provisions previously found in section 18(2) of the DPA 2018 - so that all provisions relating to the UK's regime for international transfers are now contained within Chapter 5 of the UK GDPR. This Article continues the same power for the Secretary of State to restrict, by regulations, transfers of categories of personal data to other countries or international organisations where necessary for important reasons of public interest.

SCHEDULE 6: TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES ETC: law enforcement processing

788. Chapter 5 of Part 3 of the DPA 2018 sets out the conditions under which personal data can be transferred by a competent authority, to a country outside of the UK or an international organisation, for law enforcement purposes. Schedule 6 makes various amendments to Chapter 5, to reform the UK's regime for international transfers for law enforcement purposes, as explained below.

789. Schedule 6, paragraph 2 amends section 72 of the DPA 2018, inserting additional definitions for 'relevant authority', 'relevant international organisation', 'relevant restricted transfer case' and 'overseas authoriser'. These new definitions are relevant to amendments made to section 73 and section 78.

790. Schedule 6, paragraph 3 amends section 73 of the DPA 2018, which provides that a controller may only make a transfer of personal data if the conditions of the sections are met. The general conditions for transfer remain broadly the same, with minor and technical amendments made to provide greater clarity.

Section 73 has been amended to broaden the condition previously imposed on controllers by section 73(1)(b). That provision required that where data has been received from EU Member States, prior authorisation was sought before sharing the data with a third country (apart from in specified urgent cases). These amendments remove references to EU Member States and the Law Enforcement Directive, but retain the principle, making clear that when any third country (not just EU Member States) has imposed a condition that data is not transferred further without prior authorisation, so it is regarded as a "restricted transfer case" (as defined in section 72 as amended), the UK controller must seek and obtain authorisation from the overseas authorisers before transferring personal data. There will continue to be an exception to this principle provided in subsection (5), which, as amended, will enable the controller to transfer personal data without prior authorisation where necessary to prevent an immediate and serious threat to public or national security of a third country or the UK. In such circumstances, the controller must notify the overseas authoriser as soon as reasonably practicable.

791. Schedule 6, 4 (1) omits section 74A. Previously that section provided that transfers of personal data to another country could take place where the Secretary of State had made regulations finding that the country in question provided an adequate level of protection. The free flow of personal data for law enforcement purposes would then be allowed to that country. In place of section 74A there is new section 74AA and 74AB, with amendments also made to 74B. These changes mirror those made to the equivalent provisions under the UK GDPR, in the new Articles 45A, 45B and 45C, detailed in the notes relating to Schedule 5 above, so reference should be made to those notes if a more detailed explanation on the effect of these provisions is required.

792. Section 74AA (1) provides a power for the Secretary of State to make regulations approving transfers of personal data to a third country or international organisation, thus allowing the free flow of personal data to that country or international organisation, as with the previous power to make adequacy regulations which was dealt with in section 74A of the DPA 2018. Where such regulations are in place, competent authorities will not require

any further authorisation to make a transfer of personal data to that country or international organisation, provided the transfer falls within the terms of the regulations.

793. Section 74AB sets out the data protection test which the Secretary of State must be satisfied is met in order to make regulations approving transfers to a country or international organisation. Section 74AB(1) provides that the data protection test is met if the standard of protection provided to data subjects with regard to law enforcement processing of personal data in that country or international organisation, is not materially lower than the standard of protection under Part 3 of DPA 2018 and relevant provisions in Parts 5 – 7 of that Act.

794. Section 74AB(2) sets out a list of considerations that the Secretary of State must take into account when considering whether the data protection test is met. This is a non-exhaustive list and the Secretary of State may also need to consider other matters in order to determine whether the required standard of protection exists. For example, where there are laws and practices in the third country regarding how public authorities access

personal data for national security or law enforcement purposes, to the extent that they affect the overall standard of protection, the Secretary of State will take these into account.

795. Schedule 6, (5) amends section 74B of the DPA 2018, omitting section 74B (1) and (2). Section 74B will require the Secretary of State to monitor developments in third countries and international organisations that could affect decisions to make regulations approving transfers of personal data under section 74AA, or decisions to amend or revoke such regulations. Ongoing monitoring of countries' relevant laws and practices, will enable the Secretary of State to respond to any developments that might affect decisions to make, amend or revoke regulations under section 74AA. The approach for monitoring may include, for example: dialogue with country representatives; information from HMG Embassies or High Commissions; and engagement with the Information Commissioner. Section 74B(4), as amended, sets out the actions the Secretary of State must take if the data protection test is no longer met in relation to transfers approved, or of a description approved, in regulations under

section 74AA. The Secretary of State must, to the extent necessary, either amend or revoke a regulation if the data protection test is no longer met. For example, an amendment may limit the types of transfer that are permitted by the regulation. If there is no way of amending the regulation to meet the data protection test the Secretary of State must revoke it.

796. Schedule 6 amends section 75 of the DPA 2018, which provides that transfers of personal data to third countries and jurisdictions can take place where appropriate safeguards are in place to protect that personal data. Schedule 6 introduces new subsections to this provision.

797. Paragraphs 6(1) and 6(2) of Schedule 6 are self-explanatory.

798. Paragraph 6(3) of Schedule 6 omits existing section 75(1), which currently sets out that transfers are based on appropriate safeguards where a legally binding instrument containing appropriate safeguards binds the recipient or where the controller, after assessing the circumstances surrounding the transfer, concludes that appropriate safeguards exist. Paragraph 6(4) of Schedule

6 inserts new section 75(1A) and provides that a transfer of personal data is made to a third country or international organisation subject to appropriate safeguards only if:

- the controller, acting reasonably and proportionately, considers that the data protection test is met in relation to the transfer or that type of transfer (subject to subsection (5)). This provision essentially replaces the previous section 75(1)(b);
- or (b) an appropriate legal instrument binds the intended recipient of the data (subject to new subsection (4)). This provision replicates the previous section 75(1)(a).

799. Paragraphs 6(5) and 6(6) of Schedule 6 make amendments to existing section 75(2) and 75(3), which provide further detail on controllers' obligations when relying on transfers subject to appropriate safeguards. These provisions remain largely unchanged with minor amendments to reflect the wider changes. The amendment to section 75(2) means that Controllers will be required to inform the Commissioner of the categories of data to be transferred when they rely on

section 75, whether under a legal instrument or controller determination (whereas currently notification of the Commissioner is only required where controller determination is applicable). This does not require controllers to notify the Commissioner on each occasion data is transferred, it simply requires notification of the categories of information that can take place relying on section 75.

800. Paragraph 6(7) of Schedule 6 adds new sections 75(4), 75(5), 75(6) and 76(7).

801. Paragraph 6(7) inserts a new section 75(4) which sets out the circumstances for when a legal instrument is ‘appropriate’, for the purposes of 75(1A)(b). The instrument must (a) be intended to be relied on in connection with the transfer or that type of transfer, (b) have at least one competent authority as a party to it and (c) each competent authority that is a party to it, acting reasonably and proportionately, considers that the data protection test is met in relation to the transfers, or types of transfer, intended to be made in reliance on the instrument (subject to subsection (5)). In practice, ‘appropriate legal instruments’ are likely to be agreed by government departments with their

counterparts in third countries, and that department would need to take reasonable and proportionate steps to ensure the data protection test is met. Where such instruments are in place, the Controller (assuming this is a separate entity to the party that created it) will need to ensure the data they wish to transfer is within scope of the instrument.

802. Paragraph 6(7) introduces the new data protection test in new section 75(5), which the controller or competent authority, which is party to an instrument must, acting reasonably and proportionately consider is met before a transfer under section 75 may take place. The data protection test is met, in relation to a transfer, or a type of transfer, of personal data if, after the personal data being transferred has reach its destination, the standard of protection provided for the data subject with regard to that personal data, whether by a binding legal instrument or by other means, would not be lower than the standard of the protection provided under Part 3 of the DPA 2018 and Parts 5 to 7 of the Act so far as they relate to processing by a competent authority for any of the law enforcement purposes, in a way that is material. This includes relevant enforceable

data subject rights and effective legal remedies for the data subject in all the circumstances of the transfer The new test also recognises that safeguards may be applied in different cultural and legal contexts when being used internationally and still provide appropriate protection for data subjects, and is consistent with the approach taken in the revised section 74. The reference to “other means” should be understood as anything other than a legal instrument which ensures the standard or protection and may include, for example, a situation when standard of protection is provided in the domestic laws and practices of a third country, whereby those laws would be the “other means” of protection. The test therefore does not require a point by point comparison of protections for data subjects, which would not be reasonable or proportionate given the ways in which data protection regimes may differ.

803. Paragraph 6(7) of Schedule 6 introduces new section 75(6), which provides more detail about what it means to act reasonably and proportionately. It clarifies that the actions of a controller or a competent authority that is party to an instrument must be reasonable and

proportionate in all the circumstances (or likely circumstances) of the transfer (or types of transfer) - this includes considering the nature and volume of the personal data being transferred. For example, a controller seeking to rely on the new section 75(1A)(a), is likely to have a different judgement of what is reasonable and proportionate depending on the specific transfer. If the controller seeks to transfer larger volumes of data on a more frequent basis to a specific third country, what is reasonable and proportionate is likely to be different to a more infrequent transfer. In relation to the former, the Controller may consider, for example, that it is reasonable and proportionate to establish a Memorandum of Understanding with their international counterpart to govern data transfers. which could demonstrate the steps the controller had taken, and assurances received, to ensure the protection of personal data. This process is distinct to that which the Secretary of State undertakes under new sections 74AA and 74AB. It is tailored for the purposes of controllers or competent authorities that are parties to an instrument.

804. Paragraph 6(7) of Schedule 6 introduces

new section 75(7), which clarifies that references to the protection for the data subject are to that protection taken as a whole.

805. Schedule 6, paragraph 7 amends section 76 of the DPA 2018, which provides for when data can be transferred to a third country or international organisation in the absence of 'adequacy regulations' and 'appropriate safeguards', where it is necessary for a special purpose.

806. Paragraph 7(4)(b) amends section 76(1)(c) to include reference to national security in addition to public security while also adding reference to the 'UK'. These changes ensure that Controllers are confident to transfer data where necessary for the prevention of an immediate and serious threat to national security of the UK or a third country. Paragraph 7(4)(c) and (d) make amendments to section 76(1)(d) and (e), replacing the previous wording of 'in individual cases' with 'in particular circumstances'. This new wording better reflects the fact that the law is not seeking to limit transfers by competent authorities to individual pieces of data, making clearer that transfers can take place involving a broader set or category of data in particular

circumstances. This clarity is important, as transfers of data may be particularly relevant and necessary as part of operations and investigations that are broad in scope, for example, the pursuit of child sexual abuse networks.

807. Paragraph 7(6) inserts a new additional subsection into section 76, which makes clear that controllers transferring data in reliance on section 76 must ensure that the amount of data shared is not excessive in relation to the special purpose for which it is shared. The fact that a transfer of data involves sharing multiple records would not mean that the transfer would be considered excessive, so long as the sharing is necessary and proportionate. For example, during investigations of serious and organised crime, a competent authority may conclude that it is necessary and proportionate to share multiple targeted records with a third country to help further the investigation.

808. Schedule 6, Paragraph 8 amends section 78 of the DPA 2018, which provides that where data has been transferred by a competent authority to a third country or international organisation, any subsequent transfers of that data should ordinarily take place only after the

competent authority from which the data was obtained has given its authorisation to the transfer.

809. Paragraph 8(2)(b) amends section 78 (1) so that competent authorities transferring data under Part 3 of the DPA 2018 must make it a condition of transfer that either the recipient of the data must seek prior authorisation from the UK authoriser before sharing the data further or alternatively that prior authorisation should be sought, except where the subsequent transfer is necessary to prevent an immediate and serious threat to public security or national security and there being a lack of time to reasonably seek prior authorisation. Such a transfer may occur when, for example, there is an immediate and credible threat to life such as a terrorist attack and the third country concludes that a subsequent transfer of data, originally transferred to them by a UK controller, is needed to prevent it. Where a transfer is made by the third country in such circumstances, they must notify the UK controller of such a transfer having happened as soon as reasonably practicable. It is ultimately up to the UK controller to determine whether to require prior authorisation in all

cases or whether the third country should be able to transfer without such authorisation in these limited urgent circumstances.

810. Paragraph 8(6) amends section 78(4) to broaden the principle in line with similar changes made to section 73, detailed above. Section 78(4) requires that where data has been received from EU Member States, prior authorisation was sought before the UK controller can authorise a third country to further share the data (apart from in specified urgent cases). These amendments remove references to EU Member States and the Law Enforcement Directive, but retain the principle. This makes it clear that when any third country (not just EU Member States) has imposed a condition that data is not transferred further without prior authorisation, so it is regarded as a "restricted transfer case"(as defined in section 72 as amended), the UK controller must seek and obtain authorisation from the overseas authorisers before authorising the third country to onward share the personal data. There will continue to be an exception to this principle provided in subsection (5), which, as amended, will enable the controller to transfer personal data without prior

authorisation where necessary to prevent an immediate and serious threat to the public or national security of a third country or the UK. In such circumstances, the controller must notify the overseas authoriser as soon as reasonably practicable.

811. Paragraph 8(7) amends section 78(5)(a) whereby references to member states are removed and equal consideration is given to the public security, national security or essential interests of both the UK or a third country as valid circumstances in which authorisation is not required.

SCHEDULE 7: TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES ETC: CONSEQUENTIAL AND TRANSITIONAL PROVISION

812. Part 1 of Schedule 7 makes consequential amendments to other parts of the UK GDPR and DPA 2018 which arise as a result of the changes made to the UK's regime for international transfers of personal data by Schedule 5 and Schedule 6 (as explained earlier in these Explanatory Notes).

813. Part 2 of Schedule 7 sets out transitional

provisions which are required to ensure a smooth transition between the current international transfers regime, and the new regime which will be implemented by the Bill.

814. With regard to the new regime for approving transfers of personal data to other countries and international organisations, the transitional provisions ensure that following the commencement of the new regime, transfers will continue to be allowed to any countries or international organisations which have been found adequate by the Secretary of State under the current regime, as well as to those countries and international organisations which are currently treated as adequate under Schedule 21 of the DPA 2018.

815. With regard to the new regime for transfers subject to appropriate safeguards, the transitional provisions ensure that standard data protection clauses laid by the Secretary of State under section 17C of the DPA 2018 or issued by the Commissioner under section 119A of the DPA 2018 (for example, the International Data Transfer Agreement and the EU Addendum) provide safeguards for the purposes of new Article 46(1A)(a)(i). Controllers will be able to enter into new

contracts containing the IDTA clauses to transfer personal data overseas, if the controller considers the data protection test in the new Article 46(6) of the UK GDPR is met.

816. For controllers wishing to use pre-commencement transfer mechanisms, the transitional provisions state that such mechanisms will continue to provide appropriate safeguards following commencement of the new regime if they:

- were contained in arrangements which were entered into before the new regime commences; and
- provide safeguards in accordance with Article 46(2) or (3) of the UK GDPR or paragraph 9 of Schedule 21 of the DPA 2018; or
- are a legal instrument, to which a competent authority is a party and which binds the data recipient, containing appropriate safeguards in accordance with section 75(1)(a) of the DPA 2018; and
- could validly be relied on to transfer personal data immediately before the commencement of the new regime.

817. The effect of these provisions is to allow controllers to use pre-commencement transfer mechanisms following commencement of the new regime, so long as those mechanisms satisfy the requirements of existing Article 46(1) and the last sentence of existing Article 44 of the UK GDPR, or existing section 73(3) of the DPA 2018, immediately before the regime commences. Controllers who satisfy these criteria will therefore not need to apply the new data protection test in new Article 46(6) and section 75(5) of the DPA 2018 (unless they seek to enter into new transfer mechanisms post-commencement of the Bill).

818. With regard to the new regime for derogations for specific situations, the transitional provisions also ensure that if any regulations are made by the Secretary of State under section 18(1) or 18(2) of the DPA 2018, those regulations will be treated as having been made under the restated powers in Article 49(4A) and Article 49A of the UK GDPR respectively.

SCHEDULE 8: COMPLAINTS: MINOR AND CONSEQUENTIAL AMENDMENTS

819. Schedule 8 makes consequential

amendments to the UK GDPR and the DPA 2018 relating to complaints by data subjects. These are necessary to ensure consistency as a result of changes made by new sections 164A, 164B, 165A, 165B and 166A in clauses 41 and 42.

SCHEDULE 9: DATA PROTECTION: MINOR AMENDMENTS

820. Schedule 9 makes minor miscellaneous amendments to the UK GDPR and DPA 2018, by providing definitions, removing redundant provisions and clarifying some of the pre-existing text.

SCHEDULE 10: PRIVACY AND ELECTRONIC COMMUNICATIONS: COMMISSIONER'S ENFORCEMENT POWERS

821. Regulation 31 of the current Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PEC Regulations') apply the enforcement powers in the Data Protection Act 1998 ('DPA 1998') to the PEC regulations, subject to certain modifications. These modifications are currently set out in Schedule 1 of the PEC Regulations. These provisions remain in force for the purposes of the PEC

Regulations, even though the DPA 2018 replaced the Data Protection Act 1998 for most other purposes.

822. Clause 86 substitutes Regulation 31 of the PEC Regulations with a new Regulation that makes it clear that the enforcement provisions in the DPA 2018 will now be applied to the PEC Regulations. The current Schedule 1 will also be substituted with a new Schedule 10, which makes modifications to the enforcement provisions in the DPA 2018 for the purposes of their application to the PEC Regulations.

823. Paragraph 1 of new Schedule 1 specifies the provisions in Parts 5 to 7 of the DPA 2018 that will be applied for the purposes of enforcing the PEC Regulations. They include, amongst other things, powers for the Commissioner to impose information notices, assessment notices, interview notices, enforcement and penalty notices; and the relevant rights of appeal for persons who wish to appeal against the imposition of such notices. They also include relevant criminal offences, such as the offence in section 148 of the DPA 2018 which is committed when a person deliberately frustrates an Commissioner investigation by destroying or

falsifying information. In order for these provisions to be applied to the PEC Regulations, some modifications to terminology are needed. The remaining paragraphs in this Schedule highlight where modifications are needed.

824. Paragraph 2 of Schedule 1 sets out some general modifications that are needed to the terminology in the DPA 2018, so that the enforcement provisions can be applied to the PEC Regulations. For example, any references to “the Act” or ``Parts of the Act” should be taken to mean the Act or parts of the Act as applied to the PEC Regulations.

825. Paragraphs 3 and 4 make modifications to sections 142 and 143 of the DPA 2018 on information notices for the purposes of their application to the PEC Regulations. The modifications ensure that the Commissioner can acquire relevant information and documents from a person engaged in any activity regulated by the PEC Regulations to investigate their compliance. An information notice can also be imposed on any third parties; where the third party is a communications provider the information notice can be imposed in order to determine

someone's compliance, and for all other third parties, this can be imposed when investigating a suspected breach.

826. The Commissioner will also be able to apply a duty of confidentiality (new subsection (8A) as set out in paragraph 3(c) of Schedule 1) to information notices he issues on third parties. The duty is subject to exemptions to allow disclosure of the notice (i) to employees or (ii) with permission of the Commissioner, or (iii) when obtaining legal advice. The purpose of this modification is to protect the effectiveness of the Commissioner's investigation. For example, to stop communication providers informing the relevant user (the subject of the notice) that the Commissioner is investigating them.

827. Paragraph 5 makes modifications to section 145 of the DPA 2018 on information orders for the purposes of their application to the PEC Regulations. As a result of these changes the Commissioner could apply to the court for an information order when a person fails to comply with an information notice in relation to a breach of the PEC Regulations.

828. Paragraphs 6 and 8 of Schedule 1 make

modifications to section 146 and 147 of the DPA 2018 on Assessment notices for the purposes of their application to the PEC Regulations. As a result of these modifications, the Commissioner could issue an assessment notice requiring an organisation to allow it to assess whether it has committed a breach of the PEC Regulations.

829. Clause 35 of this Bill adds new section 146A to the DPA 2018, which will allow the Commissioner to require a technical report as part of the assessment notice procedure. Paragraph 7 of new Schedule 1 sets out the modifications that are to be made to that provision for the purposes of its application to the PEC Regulations.

830. Clause 36 adds new section 148A to the DPA 2018, which will allow the Commissioner to impose an interview notice to require a person to attend an interview and answer questions when so required by the Commissioner. It also adds new section 148B which sets out some restrictions on the use of the power. Paragraphs 9 and 10 of new Schedule 1 sets out the modifications that are to be made to these provisions for the purposes of their application to the PEC

Regulations.

831. Paragraph 11 of the new Schedule 1 makes modifications to section 149 on enforcement notices for the purposes of its application to the PEC Regulations. The modifications mean that, where the Commissioner is satisfied that a person has failed, or is failing, to comply with a requirement of the PEC Regulations they may issue a written notice specifying what the person should do to remedy the failure to comply with a requirement of the PEC Regulations. The supplementary provisions in section 150 and restrictions on the use of enforcement notices in section 152 will also be modified for the purposes of the PEC Regulations via the changes in paragraphs 12 and 13 of Schedule 1.

832. Paragraph 14 of the new Schedule 1 modifies Schedule 15 (powers of entry and inspection) of the DPA 2018 for the purposes of its application to the PEC Regulations. Schedule 15 makes provision in respect of the Commissioner's powers of entry and inspection.

833. Paragraph 15 of the new Schedule 1

modifies section 155 (penalty notices) of the DPA 2018 for the purposes of its application to the PEC Regulations. 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. New subsection (1A) of section 155 provides that the Commissioner must not give a penalty notice in respect of a failure to comply with regulation 5A (personal data breach) or regulation 26A (duty to notify Commissioner of unlawful direct marketing) of the PEC Regulations, which are instead subject to a fixed monetary penalty.

834. New section (4A) of section 155 gives the Commissioner a power to give a penalty notice to an officer of a body corporate when the Commissioner has also given that body corporate a penalty notice in respect of a failure to comply with any of the requirements in regulations 19 to 24 of the PEC Regulations. This replicates the “director liability” provisions in paragraph 8AA of the current Schedule 1 to the PEC Regulations which are being replaced by this new Schedule.

835. Paragraph 16 of the new Schedule 1 modifies Schedule 16 (penalties) of the DPA

2018 for the purposes of its application to the PEC Regulations. Schedule 16 sets out procedures the Commissioner must follow when imposing a penalty notice.

836. Paragraph 17 of the new Schedule 1 makes modifications to section 156 (penalty notices: restrictions) of the DPA 2018 for the purposes of its application to the PEC Regulations. The Commissioner is prohibited from giving a penalty notice to a person who acts on behalf of either House of Parliament or to the Crown Estate Commissioners.

837. Paragraph 18 of the new Schedule 1 makes modifications to section 157 (Maximum amount of penalty) of the DPA 2018 for the purposes of its application to the PEC Regulations. This section makes provision about the maximum amount of fines that can be imposed for infringements of a provision of the PEC Regulation or a failure to comply with an information notice, interview notice, assessment notice or an enforcement notice.

838. Paragraph 18(b)(ii) lists the PEC Regulations for which a penalty notice may impose the higher maximum penalty in the event of an infringement. The higher maximum

penalty is £17,500,000 or (in the case of an undertaking) 4% of the undertaking's total annual worldwide turnover, whichever is higher. Infringement of the remaining PEC Regulations are subject to the standard maximum penalty which is £8,700,000 or (in the case of an undertaking) 2% of the undertaking's total annual worldwide turnover, whichever is higher.

839. Paragraph 19 of the new Schedule 1 modifies section 159 (amount of penalties: supplementary) of the DPA 2018 as applied for the purposes of the regulation of the PEC Regulations. This section provides the Secretary of State with the power to introduce regulations for the purposes of section 157, which make provision that a person is or is not an undertaking, that a period is or is not a financial year or about how an undertaking's turnover is to be determined. The Regulations are subject to the affirmative resolution procedure.

840. Paragraph 20 of the new Schedule 1 modifies section 160 (guidance about regulatory action) of the DPA 2018 as applied for the purposes of the regulation of the PEC Regulations. Section 160 requires the

Commissioner to produce and publish guidance about how he will exercise his functions in relation to information notices, assessment notices, interview notices, enforcement notices and penalty notices. It also sets out the procedure the Commissioner must follow for publishing the guidance and laying it in Parliament.

841. Paragraph 21 of the new Schedule 1 makes modification to section 162 (Rights of appeal) of the DPA 2018 for the purposes of its application to the PEC Regulations. This section gives a person who is given an information notice, assessment notice (including requirements relating to a technical report), interview notice, enforcement notice or penalty notice a right to appeal against that notice/requirement. A person whose application for the cancellation or variation of an enforcement notice is refused is given a right to appeal against that refusal. This section also 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.

842. Paragraph 22 of the new Schedule 1 makes modification to section 163

(Determination of appeals) of the DPA 2018 for the purposes of its application to the PEC Regulations. This section makes provision in relation to the determination of appeals under section 162 by the Upper Tribunal or the First-tier Tribunal.

843. Paragraph 23 of the new Schedule 1 makes modification to section 180 (Jurisdiction) of the DPA 2018 for the purposes of its application to the PEC Regulations. This section sets out which courts have jurisdiction for information orders. 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. An exception is made for cases in which the information notice contains an urgency statement or there is an application to challenge urgent notices under section 164, when only the High Court or, in Scotland, the Court of Session can make an information order.

844. Paragraph 24 of the new Schedule 1 makes modification to section 181 (Interpretation of Part 6) of the DPA 2018 for the purposes of its application to the PEC Regulations.

845. Paragraph 25 and 26 of the new Schedule 1 make modification to section 182 (Regulations and consultation) of the DPA 2018 for the purposes of its application to the PEC Regulations. This section makes provision concerning the form, process and procedure for making regulations under the powers in the DPA 2018 (as applied), including consultation requirements.

846. Paragraph 27 of the new Schedule 1 makes modification to section 196 (Penalties for offences) of the DPA 2018 for the purpose of its application to the PEC Regulations. Where offences relate to a person's frustration or obstruction of the Commissioner's investigations of breaches of the PEC Regulations, the penalties that can be imposed by the courts will be identical to those that apply when the offence relates to obstruction of investigations for breaches of the data protection legislation.

847. Paragraph 28 of the new Schedule 1 makes modification to section 200 (Guidance about PACE codes of practice) of the DPA 2018 for the purpose of its application to the PEC Regulations. Section 200 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). The modifications made by paragraph 28 are self-explanatory.

848. Paragraph 29 of the new Schedule 1 makes modification to section 202 (Proceedings in the First-tier Tribunal: contempt) of the DPA 2018 as applied for the purposes of the regulation of the PEC Regulations. 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. The modifications made by paragraph 29 are self-explanatory.

849. Paragraph 30 of the new Schedule 1 modifies section 203 (Tribunal procedure rules) of the DPA 2018 for the purposes of its application to the PEC Regulations. This section sets out the power to make Tribunal Procedure Rules to regulate the way the rights of appeal conferred by section 162 are

exercised.

850. Paragraph 31 is self-explanatory.

SCHEDULE 11: REGISTERS OF BIRTHS AND DEATHS: MINOR AND CONSEQUENTIAL AMENDMENTS

851. Part 1 makes a number of amendments to the BDRA including: amending sections of the BDRA which referred to “the registrar or superintendent registrar as having custody of the register” and replacing such references with “appropriate registration officer for the register”. Other amendments specify how indexes need to be created and retained by both the Registrar General and the superintendent registrar.

852. Part 2 makes minor and consequential amendments to other primary legislation as a result of the changes to the registration system brought about by this Bill

SCHEDULE 12: INFORMATION STANDARDS FOR HEALTH AND ADULT SOCIAL CARE IN ENGLAND

853. Schedule 12 amends section 250 (powers to publish information standards) of the Health and Social Care Act 2012 (HSCA 2012).

854. Paragraph 3(2) amends section 250(2) to make clear that an information standard (a standard in relation to the processing of information) that may be prepared and published under section 250(1) includes a standard relating to information technology (IT) or IT services used or intended to be used in connection with the processing of information.

855. Paragraph (3) makes a technical amendment to section 250(2B) to ensure that an information standard may apply to a public body which exercises functions in connection with the provision in relation to (as well as in) England of health care or of adult social care. This reflects the fact that, by virtue of section 250(2B) of the HSCA 2012, the persons to whom information standards may apply include persons who are required to be registered (with the Care Quality Commission) in respect of the carrying on of a regulated activity: under

the Health and Social Care Act 2008, an activity may be prescribed as a “regulated activity” if, amongst other things, it involves, or is connected with, the provision of health or social care in, or in relation to, England.

856. Paragraph 3(4) amends section 250(2B) by adding relevant IT providers to the list of persons to whom an information standard may apply (the definition of a “relevant IT provider” is explained below).

857. Paragraph 3(5) makes a technical amendment to section 250(3) to make it clear that the Secretary of State’s power, under section 250(1), to prepare information standards may be exercised in relation to information concerning, or connected with, the provision of health and adult social care in relation to England (as well as in England). As above, this reflects the fact that, by virtue of section 250(2B) of the HSCA 2012, the persons to whom information standards may apply include persons who are required to be registered (with the Care Quality Commission) in respect of the carrying on of an activity which involves, or is connected with, the provision of health or social care in, or in relation to, England.

858. Paragraph 3(6) makes a technical amendment to section 250(7) so that the definitions in that subsection apply for the purposes of the entirety of Chapter 1 of Part 9 of the HSCA 2012, rather than just section 250 in that Chapter.

859. Paragraph 3(6) inserts definitions of "information technology", "IT service" and "relevant IT provider" into section 250(7). "Information technology" includes IT products such as computers, other devices whose uses include the processing of information by electronic means ("IT devices"); parts, accessories and other equipment made or adapted for use in connection with computers or IT devices; software and code made or adapted for use in connection with computers or IT devices; and networks and other infrastructure (whether physical or virtual) used in connection with other IT. "IT service" means a physical or virtual service consisting of, or provided in connection with, developing, making available, operating or maintaining information technology. "Relevant IT provider" means a person involved in marketing, supplying, providing or otherwise making available IT, IT services or a service which

consists of processing information using IT, for payment or free of charge, so far as the IT or service is used, or intended for use, in connection with the provision in or in relation to England of health or adult social care.

860. Paragraph 3(6) also makes a technical amendment to the definition of "processing" in section 250(7) to omit a reference to section 3(14) of the DPA 2018 which glosses references to the processing of personal data and which is unnecessary in light of the fact that section 250 does not refer to the processing of personal data.

861. Paragraph 4 of Schedule 12 inserts new section 250A into the HSCA 2012. New subsection (1) enables an information standard to make provision about the design, quality, capabilities or other characteristics of IT or IT services. Information standards can also make provision about contracts or other arrangements under which IT or IT services are marketed, supplied, provided or otherwise made available.

862. New subsection (2) of section 250A enables an information standard to make technical provision about IT and IT services.

This can include provision about:

- functionality (e.g. how an IT product or service works to provide the desired outcome);
- connectivity (e.g. the ability of an IT product or service to connect with other computer systems or application programs);
- interoperability (e.g. how IT products or services from different providers exchange or share information);
- portability (e.g. the possibility of the IT product or service to be used in different environments without required significant rework);
- storage of, and access to information (e.g. how, where and why information is stored, and the format in which it is stored);
- the security of information (e.g. the processes and methodologies involved with keeping information confidential yet accessible where appropriate, and assuring its integrity).

863. New subsection (3) of section 250A

provides that an information standard can make provision by reference to open standards or proprietary standards. This could include standards produced by standards development organisations.

864. Paragraph 5 of Schedule 12 substitutes subsection (3) of section 251 of the HSCA 2012. Section 251(3) enables the Secretary of State or NHS England to adopt an information standard prepared or published by another person. The substituted subsection (3) ensures that this extends to information standards as they have effect from time to time, and that information standards can make provision by reference to international agreements or other documents (including as they have effect from time to time). Paragraph 5 also makes a consequential amendment to the heading of section 251.

865. Paragraph 6 of Schedule 12 inserts a new heading “Compliance with Standards” after section 251. Paragraph 7 substitutes the heading of section 251ZA. Paragraph 8 inserts new sections 251ZB, 251ZC, 251ZD and 251ZE after section 251ZA.

866. New section 251ZB(1) provides that if the

Secretary of State has reasonable grounds to suspect that a relevant IT provider is not complying with an information standard that applies to the IT provider, the Secretary of State may give the IT provider a written notice which identifies the information standard in question, sets out the grounds for suspecting non-compliance, asks the IT provider to comply within a specified period, asks the IT provider to provide evidence of compliance within a specified period, and where appropriate sets out the steps that the IT provider must take within a specified period in order to comply with the standard.

867. Section 251ZB(2) sets out that any period specified for the purposes of subsection (1) must be at least 28 days beginning with the day the notice is given.

868. Section 251ZB(3) provides that the Secretary of State may vary or revoke a notice given to a relevant IT provider under section 251ZB(1) by means of a further written notice.

869. New section 251ZC provides for public censure of a relevant IT provider in certain circumstances. Subsection (1) provides that, if the Secretary of State has reasonable grounds

to suspect an IT provider is not complying with an information standard that applies to the IT provider, the Secretary of State can publish a statement to that effect.

870. Subsection (2) provides that the published statement can include the text of the notice given to an IT provider under section 251ZB (notice requesting compliance).

871. Subsection (3) stipulates that before a statement is published under section 251ZC, the Secretary of State must give the relevant IT provider a copy of the terms of the proposed statement, and an opportunity to make representations about the decision to publish a statement and the terms of the statement.

872. Subsection (4) stipulates that if the Secretary of State decides to publish the statement after considering any representations made by the relevant IT provider, the Secretary of State must inform the IT provider before publishing the statement.

873. New section 251ZD enables the Secretary of State to delegate certain functions to other persons. Those functions are listed in subsection (3) and consist of functions under

section 251ZA (monitoring compliance), so far as they relate to relevant IT providers, and functions under section 251ZB (notice requesting compliance). Subsection (1) provides that the Secretary of State may direct a public body to exercise some or all of those functions and give the public body directions about the exercise of those functions.

874. Subsection (2) enables the Secretary of State to make arrangements for a person prescribed by regulations to exercise some or all of those functions.

875. Subsection (4) enables the arrangements made under subsection (2) to provide for the making of payments to the person with whom the arrangements are made, and to make provision about the circumstances in which such payments are to be repaid to the Secretary of State.

876. New section 251ZE provides for the accreditation of IT and IT services. Subsection (1) enables regulations to make provision for the establishment and operation of a scheme for accreditation of IT and IT services.

877. Subsection (2) enables the regulations to provide for the scheme to be established and

operated by a person ("operator") specified in the regulations.

878. Subsection (3) enables the regulations to, among other things, confer power on the operator to establish the procedure for accrediting IT and IT services under the scheme, set the criteria for accreditation (the accreditation criteria), to keep an accreditation under the scheme under review and to charge a reasonable fee in respect of an application for accreditation.

879. Subsection (4) enables the regulations to, among other things, make provision that requires the operator of the accreditation scheme to set some or all of the accreditation criteria by reference to information standards, to publish details of the scheme including the accreditation criteria, to provide for the review of a decision to refuse an application for accreditation, and to provide advice to applicants for accreditation with a view to ensuring that the accreditation criteria are met.

SCHEDULE 13: THE INFORMATION COMMISSION

880. Paragraph 1 of Schedule 13 inserts a new

Schedule 12A into the DPA 2018 which describes the nature, form and governance structure of the new body corporate (the Information Commission).

881. Paragraph 2 of Schedule 13 contains transitional provisions. It makes provision that the person who holds the office of Information Commissioner immediately before the day on which the Schedule comes into force is to be treated as having been appointed as the chair of the Information Commission for a term that expires at the time the person would cease to hold the office of Information Commissioner but for its abolition.

NEW SCHEDULE 12A TO THE DATA PROTECTION ACT 2018: THE INFORMATION COMMISSION

882. Paragraph 1 states that the Information Commission is not to be regarded as a servant or agent of the Crown, or as enjoying any status, immunity or privilege of the Crown. The Commission's property is not to be regarded as property of, or property held on behalf of, the Crown.

883. Paragraph 2 prescribes that the number of

members of the Information Commission must not be less than 3, or more than 14. It confers power on the Secretary of State to change the maximum number of members of the Commission via regulations, which will be subject to the negative resolution procedure.

884. Paragraph 3 makes provision for the membership of the Commission.

885. Paragraph 4 stipulates that the Secretary of State must exercise the powers in paragraphs 2 and 3 to ensure that, in so far as practicable, non-executive members outnumber executive members.

886. Paragraph 5 requires that the chair and other members of the Commission are selected on merit on the basis of fair and open competition.

887. Paragraph 6 makes provision for conflicts of interest.

888. Paragraph 7 makes provision for the tenure of the chair.

889. Paragraph 8 makes provision for the tenure of the deputy chair.

890. Paragraph 9 makes provision for the

tenure of the other non-executive members.

891. Paragraph 10 makes provision for the remuneration and pensions of the non-executive members.

892. Paragraph 11 makes provision in relation to the terms and conditions of the executive members.

893. Paragraph 12 makes provision for the appointment and in relation to the terms and conditions of other staff of the Information Commission.

894. Paragraph 13 makes provision in relation to committees of the Commission.

895. Paragraph 14 makes provision in relation to the delegation of functions of the Commission.

896. Paragraph 15 makes provision regarding advice from committees.

897. Paragraph 16 makes provision in relation to proceedings of the Commission and its committees.

898. Paragraph 17 requires that the Commission makes arrangements for the keeping of records of proceedings.

899. Paragraph 18 makes provision for disqualification for acting in relation to certain matters.

900. Paragraph 19 makes provision regarding the validity of proceedings of the Commission, of the non-executive members of the Commission and of committees of the Commission.

901. Paragraph 20 provides that the Secretary of State may make payments to the Commission.

902. Paragraph 21 makes provision regarding fees, charges, penalties and other sums received by the Commission in carrying out its functions.

903. Paragraph 22 makes provision concerning the keeping of accounts.

904. Paragraph 23 makes provision about the authentication of the Information Commission's seal and the presumption of the authenticity of documents.

905. Paragraph 24 makes transitional provision for the appointment of an interim chief executive.

906. Paragraph 25 relates to the interpretation of references to pensions, allowances and gratuities.

Commencement

907. The majority of provisions in this Bill will be brought into force by regulations made by the Secretary of State.

908. Clauses 64, 79 and Part 6 of the Bill will come into force on Royal Assent, as will any powers that are needed to make regulations.

909. The following provisions will come into force two months after Royal Assent:

- Clause 4 (consent to law enforcement processing);
- Clause 14 (representatives of controllers or processors not established in the UK);
- Clause 17 (logging of law enforcement processing);
- Clause 36 (power of Commissioner to require documents);
- Clause 113 (oversight of biometrics databases).

Financial implications of the Bill

Data Protection and Digital Verification Services

910. In the Impact Assessment published in March 2023, the government estimates the Net Present Social Value of all of the reforms to be approximately £4.7 billion across the 10 years after implementation in 2024, in 2019 prices.

911. The majority of the benefit to the public sector will come from the reforms aimed at the use of data for Law Enforcement and National Security and Digital Verification Services. DSIT estimates the total Net Present Impact on public expenditure to be £0.3bn over 10 years, in 2019 prices with a 2020 base year.

912. Costs for the Commissioner are expected to increase especially as they familiarise and adapt to the new legislation. The government also expects an increase in regulator costs associated with the Digital Verification Services measures. All these costs form part of current budget arrangements.

913. The Net Present Value to the Private Sector of all of the reforms in the bill is expected to be approximately £2.2 billion over the course of the 10 years after

implementation in 2024 and in 2019 prices. The majority of these cost savings come from Digital Verification Services and Data Protection measures which are expected to decrease compliance costs and increase productivity levels within the economy.

914. The majority of amendments made at committee stage do not have any additional economic or wider impacts to UK businesses, the public sector or data subjects above what is already included in the Impact Assessment. For substantial technical and policy amendments that have potential impact we have included an outline of the rationale, purpose and impact of these in our analytical note. A fully updated economic Impact Assessment will be provided at Royal Assent, as per RPC guidance.

Enforcement provisions

915. It is estimated that the logging proposal could bring benefits for law enforcement agencies in the range of £64.5 to £1,319.1 million (Present Value), with a central estimate of £400.2 million (PV) over 10 years from 2024 in 2021 prices. It is estimated that the proposal to permit the active human review of

automated decisions could cost up to £0.17 million (PV), with a central estimate of £0.03 million (PV) over 10 years.

Registers of births and deaths

916. It is estimated that the set-up costs for the General Register Office and the local registration service of moving from paper-based birth and death registers to an electronic register will be approximately £0.1m. The reforms of the birth and death registration system are expected to lead to total net savings of approximately £18.1m (PV) over 10 years from 2024 to 2034 in 2021 prices.

Extending data sharing powers under section 35 of the Digital Economy Act 2017

917. There will be little or no direct financial costs or benefits of the extension of data sharing powers. The impacts will be experienced when public authorities use these powers to share data in order to support government services for businesses.

Health and Adult Social Care System

918. The information standards measures in this Bill are, in the most part, enabling provisions and are available in relation to information technology (IT) providers who make IT, IT services or information processing services using IT available in connection with health or adult social care provision in, or in relation to, England. As a result most of the proposals will not place direct costs on health or adult social care organisations purely by their enactment. Where costs are incurred, many will only materialise at a later stage depending on how the powers are used and how the provisions are deployed. Where some of the proposals trigger costs, these are expected to be limited and in relation to which funding will be considered with benefits to the organisation's wider activities. As such, it is difficult to monetise any costs at this stage.

919. The provisions in the Bill that may result in small costs to the health and adult social care system include, but are not limited to:

- the imposition of new information standards on IT providers supplying IT to the health and social care sector, including communications to existing IT providers and administration associated with

reviewing current contracts or entering new contracts;

- the establishment and operation of a compliance function to monitor compliance with information standards by IT providers, including data collection where required;
- the establishment and operation of an accreditation scheme.

Smart Data schemes

920. The provisions on Smart Data in Part 3 includes provisions for regulations to impose fees on data holders and others (Clause 74) and to impose a levy on data holders. These are intended to cover the costs incurred by decision-makers and enforcers in exercising their functions.

921. These provisions aim to ensure schemes are self-funding and not reliant on public funds.

Parliamentary approval for financial costs or for charges imposed

922. The Bill requires a money resolution because it gives rise to charges on the public revenue (that is, broadly speaking, new public expenditure). The money resolution covers:

- expenditure by the Secretary of State and the Treasury under various provisions of the bill, including clause 76 , which enables the Secretary of State and the Treasury to provide financial assistance to certain persons in connection with regulations about access to customer data and business data made under Part 3 of the bill, and Schedule 13, which enables the Secretary of State to make payments to the Information Commission (paragraph 20 of new Schedule 12A to the Data Protection Act 2018);
- expenditure by government departments and other public bodies in complying with new requirements under the data protection legislation;
- other increases in public expenditure under other Acts - for example, under

paragraph 9 of Schedule 12 to the Data Protection Act 2018 (payments by the Secretary of State to the Information Commissioner, prior to that office being replaced by the Information Commission).

923. The Bill requires a ways and means resolution because it authorises new charges on the people (that is, broadly speaking, new taxation or other similar charges). The ways and means resolution covers:

- the charging of fees under clause 52, which enables the Secretary of State to charge fees in connection with registration in the verification services register;
- the charging of fees, and the imposition of a levy, for the purposes of meeting expenses incurred in connection with regulations about access to customer data and business data made under Part 3 of the bill (see clauses 74 and 75).

924. These motions were agreed by the House of Commons on 17 April 2023.

Compatibility with the European Convention on Human Rights

925. The Secretary of State, Michelle Donelan, has made a statement pursuant to section 19 of the Human Rights Act 1998 that, in her view, the provisions of the Data Protection and Digital Information Bill are compatible with the rights under the European Convention on Human Rights.

926. Issues arising as to the compatibility of the Bill with the Convention rights are dealt with in a separate memorandum. This will be published separately on gov.uk on 8 November 2023.

No statement under the Environment Act 2021

927. The Secretary of State, Michelle Donelan, is of the view that the Bill as introduced into the House of Commons does not contain provision which, if enacted, would be environmental law for the purposes of section 20 of the Environment Act 2021.

Related documents

928. The following documents are relevant to the Bill and can be read at the stated locations:

- Data Protection Act 2018

  https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

- Privacy and Electronic Communications Regulations 2003 https://www.legislation.gov.uk/uksi/2003/2426/contents/made

- Data: A New Direction consultation and government response https://www.gov.uk/government/consultations/data-a-new-direction

- Legislative and Regulatory Reform Act 2006 https://www.legislation.gov.uk/ukpga/2006/51/contents

- Deregulation Act 2015 https://www.legislation.gov.uk/ukpga/2015/20/section/108/enacted

- UK digital identity and attributes trust framework beta - https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-

framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version

- DHSC: Health and Care Act 2022 - https://www.legislation.gov.uk/ukpga/2022/31/pdfs/ukpga_20220031_en.pdf
- DHSC: Health and Care Act 2022 - Explanatory notes https://publications.parliament.uk/pa/bills/cbill/58-02/0140/en/210140en.pdf
- DHSC: Health and Social Care Act 2012 - https://www.legislation.gov.uk/ukpga/2012/7/contents/enacted
- DHSC: Health and Social Care Act 2012 - Explanatory notes - https://www.legislation.gov.uk/ukpga/2012/7/notes/contents
- DHSC: Data saves lives: reshaping health and social care with data https://www.gov.uk/government/publications/data-saves-lives-reshaping-health-and-social-care-with-data
- NHS Long Term Plan: NHS Long Term Plan [online version] https://www.longtermplan.nhs.uk/online-version/

- DHSC: A plan for digital health and social care A plan for digital health and social care https://www.gov.uk/government/publications/a-plan-for-digital-health-and-social-care/a-plan-for-digital-health-and-social-care
- Smart Data Review (consultation), 2018 https://www.gov.uk/government/publications/smart-data-review
- Smart Data: putting consumers in control of their data (consultation response), 2019 https://www.gov.uk/government/consultations/smart-data-putting-consumers-in-control-of-their-data-and-enabling-innovation
- Smart Data Working Group: Spring 2021 Report https://www.gov.uk/government/publications/smart-data-working-group-spring-2021-report
- FCA Open finance – feedback statement https://www.fca.org.uk/publications/feedback-statements/fs21-7-open-finance-feedback-statement
- FCA Open finance – feedback statementhttps://www.fca.org.uk/publications/feedback-statements/fs21-7-open-finance-

feedback-statement

- Digital Economy Act 2017 https://www.legislation.gov.uk/ukpga/2017/30/section/43/enacted
- Digital Economy Act 2017 Codes of Practice https://www.gov.uk/government/publications/digital-economy-act-2017-part-5-codes-of-practice
- Digital Economy Act 2017 - Explanatory Notes https://www.legislation.gov.uk/ukpga/2017/30/notes
- Codes of Conduct (guidance published by ICO in relation to UK GDPR) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct
- Lords Committee on Justice and Home Affairs report - 'The advent of new technologies in the justice system'. https://publications.parliament.uk/pa/ld5802/ldselect/ldjusthom/180/18002.htm
- Lords European Union Committee report - 'Beyond Brexit: policing, law enforcement

and security' https://committees.parliament.uk/publications/5298/documents/52902/default/

- Justice and Home Affairs Committee, 'Technology Rules? The advent of new technologies in the justice system' https://publications.parliament.uk/pa/ld5802/ldselect/ldjusthom/180/18002.htm

Annex A - Territorial extent and application in the United Kingdom

Provision	England	Wales		Scotland		Northern Ireland	
	Extends to E & W and applies to England	**Extends to E & W and applies to Wales**	**Legislative Consent Process engaged?**	**Extends and applies to Scotland?**	**Legislative Consent Motion process engaged?**	**Extends and applies to Northern Ireland?**	**Legislative Consent Motion process engaged?**
Part 1: DATA PROTECTION							
Definitions							
Clause 1	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 2	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 3	Yes	Yes	N/A	Yes	N/A	Yes	N/A

Clause 4	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Data protection principles							
Clause 5	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 6	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Special categories of personal data							
Clause 7	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Data subjects' rights							
Clause 8	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 9	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 10	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 11	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Automated decision-making							
Clause 12	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Obligations of controllers and processors							
Clause 13	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 14	Yes	Yes	N/A	Yes	N/A	Yes	N/A

Clause 15	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 16	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 17	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 18	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 19	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 20	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 21	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 20	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 22	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 23	Yes	Yes	N/A	Yes	N/A	Yes	N/A
International transfers of personal data							
Clause 23	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Safeguards for processing for research etc purposes							
Clause 24	Yes	Yes	N/A	Yes	N/A	Yes	N/A

Clause 25	Yes	Yes	N/A	Yes	N/A	Yes	N/A
National security							
Clause 26	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Intelligence services							
Clause 27	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 28	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Information Commissioner's role							
Clause 29	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 30	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 31	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 32	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 33	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 34	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 35	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Enforcement							

Clause 36	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 37	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 38	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 39	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 40	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 41	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 42	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 43	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 44	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Protection of prohibitions, restrictions and data subject's rights							
Clause 45	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Miscellaneous							
Clause 46	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 47	Yes	Yes	N/A	Yes	N/A	Yes	N/A

Part 2: DIGITAL VERIFICATION SERVICES							
Introductory							
Clause 48	Yes	Yes	N/A	Yes	N/A	Yes	N/A
DVS trust framework							
Clause 49	Yes	Yes	N/A	Yes	N/A	Yes	N/A
DVS register							
Clause 50	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 51	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 52	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 53	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 54	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 55	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Information gateway							
Clause 56	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 57	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 58	Yes	Yes	N/A	Yes	N/A	Yes	N/A

Clause 59	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 60	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Trust mark							
Clause 61	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Supplementary							
Clause 62	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 63	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 64	Yes	Yes	N/A	Yes	N/A	Yes	N/A
PART 3: CUSTOMER DATA AND BUSINESS DATA							
Clause 65	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 66	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 67	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 68	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 69	Yes	Yes	In part	Yes	In part	Yes	Yes

Clause 70	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 71	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 72	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 73	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 74	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 75	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 76	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 77	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 78	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 79	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 80	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 81	Yes	Yes	In part	Yes	In part	Yes	Yes

Part 4: OTHER PROVISION ABOUT DIGITAL INFORMATION							
Privacy and electronic communications							
Clause 82	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 83	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 84	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 85	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 86	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 87	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 88	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 89	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 90	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 91	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Claus	Yes	Yes	N/A	Yes	N/A	Yes	N/A

e 92							
Trust services							
Clause 93	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 94	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 95	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 96	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 97	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Sharing of information							
Clause 98	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Clause 99	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Clause 100	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Registers of births and deaths							
Claus	Yes	Yes	N/A	No	N/A	No	N/A

e 101							
Clause 102	Yes	Yes	N/A	No	N/A	No	N/A
Clause 103	Yes	Yes	N/A	No	N/A	No	N/A
Clause 104	Yes	Yes	N/A	No	N/A	No	N/A
Clause 105	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Information standards for health and social care							
Clause 106	Yes	No	N/A	No	N/A	No	N/A
Part 5: REGULATION AND OVERSIGHT							
Information Commission							
Clause 107	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 108	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 109	Yes	Yes	N/A	Yes	N/A	Yes	N/A

Clause 110	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Oversight of biometric data							
Clause 111	Yes	Yes	No	In part	No	In part	No
Clause 112	Yes	Yes	N/A	No	N/A	No	N/A
Clause 113	Yes	Yes	N/A	No	N/A	No	N/A
Part 6: FINAL PROVISIONS							
Clause 114	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 115	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 116	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 117	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Claus	Yes	Yes	N/A	Yes	N/A	Yes	N/A

e 118							
Clause 119	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 120	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 121	Yes	Yes	N/A	Yes	N/A	Yes	N/A
SCHEDULES							
Schedule 1	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Schedule 2	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Schedule 3	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Schedule 4	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Schedule 5	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Schedule 6	Yes	Yes	N/A	Yes	N/A	Yes	N/A

Schedule 7	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Schedule 8	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Schedule 9	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Schedule 10	Yes	Yes	N/A	In part	N/A	In part	N/A
Schedule 11	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Schedule 12	Yes	No	N/A	No	N/A	No	N/A
Schedule 13	Yes	Yes	N/A	Yes	N/A	Yes	N/A

Subject matter and legislative competence of devolved legislatures

Data protection

929. The Bill's data protection provisions in Part 1, and provisions in relation to the Information Commission in Part 5, extend to the whole of the UK, apart from one provision relating to the Information Commission's seal, which does not extend to Scotland. The data protection reservations in relation to Scotland, Wales and Northern Ireland apply for these provisions.

Privacy and Electronic Communications Regulations

930. Changes to the Privacy and Electronic Communications (EC Directive) Regulations 2003 in Part 4 extend to the whole of the UK. The telecommunications reservations in relation to Scotland, Wales and Northern Ireland apply for these provisions.

Police use of biometrics

931. Changes to police use of biometrics and overt surveillance are limited to England and Wales[12].

Implementation of law enforcement information sharing-agreements

[12] The only exception to this is the changes to the oversight of National Security Determinations (applications submitted under s63M of PACE) which will apply UK wide as national security matters are reserved.

932. The territorial extent of these provisions is UK wide. International agreements are reserved by the UK Government as prerogative powers to be excised by the Secretary of State. The implementation of such agreements is devolved. As a result, a LCM will be required from Scotland, Wales and Northern Ireland.

Registers of Births and Deaths

933. Legislative competence for births and deaths (and civil registration generally) is devolved to Scotland and Northern Ireland and separate legislation exists to govern the registration of births and deaths in those jurisdictions. Legislative competence in respect of civil registration is not devolved in Wales.

934. The clauses which amend the Births and Deaths Registration Act 1953 and the Registration Service Act 1953, relating to the registration of births and deaths in England and Wales extend and apply to England and Wales only.

935. These provisions also give effect to minor and consequential amendments which do not change the application of the law in Scotland and Northern Ireland, but the extent of the

provisions amended applies to Scotland and Northern Ireland.

936. Provisions in the Bill which enable regulations to make amendments to primary and secondary legislation in consequence of the changes made to birth and death registration in England and Wales extend to the whole of the UK.

Digital Verification Services

937. The territorial extent of these provisions is UK wide.

938. The telecommunications reservation in relation to Scotland, Wales and Northern Ireland applies to digital verification services.

Trust Services

939. The territorial extent of these provisions is UK wide.

Extending data sharing powers under section 35 of the Digital Economy Act 2017

940. The territorial extent and application of these provisions is UK wide. Like section 35 of the DEA 2017, this provision will extend and apply to the UK (though the powers in Part 5,

chapter 1 of the DEA 2017 have yet to be commenced in Northern Ireland).

941. There is no relevant reservation for the power in this provision so a LCM is required. The clause relates to public service delivery to businesses which is not solely for reserved purposes but also for devolved purposes, such as providing devolved public services to businesses. The clause will also alter the executive competence of the Devolved Administrations by extending the scope of their regulation-making powers. It will do this by widening the conditions with which an objective must comply in order to meet the definition of an information-sharing "specified objective" to improve public service delivery under section 35 (9) – (12) of the DEA 2017 by adding public service delivered to businesses.

Health and Adult Social Care System

942. The territorial extent of these provisions is England and Wales only.

Smart Data schemes

943. The territorial extent of these provisions is UK wide. The legislation applies to businesses operating in the UK.

944. While many aspects of the proposals are reserved, some areas are devolved (e.g. where the customer is a business and not an individual), and consumer protection in Northern Ireland. Therefore a LCM is required in all three Devolved Administrations.

DATA PROTECTION AND DIGITAL INFORMATION BILL

EXPLANATORY NOTES

These Explanatory Notes relate to the Data Protection and Digital Information Bill, as introduced in the House of Commons on 8 November 2023.

Ordered by the House of Commons to be printed, 8 November 2023

PUBLISHED BY AUTHORITY OF **THE HOUSE OF COMMONS**