DATA (USE AND ACCESS) BILL [HL]

EXPLANATORY NOTES

What these notes do

These Explanatory Notes relate to the Data (Use and Access) Bill [HL] as introduced in the House of Lords on 23 October 2024 (HL Bill 40).

- These Explanatory Notes have been prepared by the Department for Science, Innovation and Technology, Department of Health and Social Care, the Home Office, the Department for Business and Trade, HM Treasury, and the Department for Energy Security and Net Zero, in order to assist the reader of the Bill and to help inform debate on it. They do not form part of the Bill and have not been endorsed by Parliament.
- These Explanatory Notes explain what each part of the Bill will mean in practice; provide background information on the development of policy; and provide additional information on how the Bill will affect existing legislation in this area.
- These Explanatory Notes might best be read alongside the Bill. They are not, and are not intended to be, a comprehensive description of the Bill.

Table of Contents

Overview of the Bill

1 This Bill is intended to harness the power of data for economic growth, support a modern digital government, and improve people's lives.

2 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 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.

3 The Bill establishes a legislative structure for the provision of digital verification services in the United Kingdom (UK), where providers of those services wish to be registered on a government register. This structure aims to enable users to recognise trusted digital identity providers within the digital identity market and enable digital identities and attributes to be used with the same confidence as paper documents. These measures make provision for the preparation and publication of a trust framework of rules concerning the provision of digital verification services, together with supplementary rules (known as supplementary codes) for specific use cases. They also establish a publicly available register of persons providing digital verification services that are certified against those rules and supplementary rules (if applicable). Finally, they provide that registered persons can use a trust mark and have access to an information gateway, to enable public authorities to disclose personal information to registered persons for identity and eligibility verification purposes.

4 The Bill includes provisions which provide a legislative framework to support the operation of the National Underground Asset Register, a digital map that will improve both the efficiency and safety of underground work by providing secure access to location data about pipes, cables and other types of apparatus installed in streets.

5 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.

6 Targeted reforms to parts of the UK's data protection and privacy framework will maintain high standards of protection, whilst addressing a lack of clarity in existing legislation that impedes the safe development and deployment of some new technologies. These reforms are intended to support economic growth and a modern digital government.

7 The Bill includes provisions facilitating the flow and use of personal data for law enforcement and national security purposes. These reforms seek to enhance the work of law enforcement and national security agencies in the interest of public security. Provisions also seek to improve law enforcement efficiency by removing unnecessary complexity and processes, and reducing differences across the data processing regimes.

8 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. These reforms are intended to give the regulator new, stronger powers and a more modern structure – while maintaining its independence.

9 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.

10 The Bill is intended to provide the Gas and Electricity Markets Authority flexibility to determine the best process to follow in appointing the successor licensee for providing smart meter communication services. It follows a review of the current licensing process by the Office of Gas and Electricity Markets (Ofgem), being the body that supports the Authority.

11 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.

12 The Bill makes amendments to the Online Safety Act 2023 to create a requirement for OFCOM, when notified of a child death by the Coroner (or Procurator Fiscal in Scotland) to issue an information notice to specified online service providers requiring them to retain certain information relating to the use of the service by the deceased child for a specified period.

13 The Bill provides a regulation-making power to create a framework allowing researchers access to data relating to online safety held by tech companies.

14 The Bill makes provision for the retention of biometric information, including that received through international partner sharing, with the intention of improving efficiency and limiting risk to national security.

15 The Bill then includes provisions which seek to update regulations to make sure that the UK's trust services legal framework continues to function effectively.

Policy background

16 The Government wants to harness the power of data for economic growth, to support a modern digital government, and to improve people's lives. The Data (Use and Access) Bill has been designed with the intention of achieving these 3 objectives.

17 The UK data economy (its data market plus the value data adds to other sectors of the economy) represents an estimated 6.9 per cent of GDP (as of 2022). Data is essential to UK businesses: 77 percent of UK businesses handle some form of digital data; increasing to 99 percent for businesses employing more than 10 people. In 2021, data-enabled UK service exports accounted for 85 per cent of total service exports, estimated to be worth £259 billion.

Access to customer data and business data

18 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.

19 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.

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

- rebalancing the information asymmetry between suppliers and customers;
- 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 lower prices and higher quality goods and service delivery; and
- providing new services in and across the sectors, such as those which may help consumers save and manage their money and services.

21 Open Banking is the only active example of a regime that is comparable to a 'Smart Data scheme' – but needs a legislative framework to put it on a permanent footing, from which it can grow and expand. In 2017, following a market investigation due to competition concerns, the CMA ordered the nine biggest banking providers in the UK to 'open up' the data relating to personal and business current accounts. The CMA required the nine largest banking providers to set up the Open Banking Implementation Entity to oversee the scheme. In January 2023 the CMA announced the substantial completion of the Open Banking roadmap, with focus shifting towards preparing for the transition to new arrangements for Open Banking. As of July 2024, there are over 10 million consumers and small businesses using Open Banking.

Digital Verification Services

22 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 establishes a legislative structure for the provision of digital verification services in the UK, where providers of those services wish to be registered on a government register. It also enables public authorities to disclose personal information to registered digital verification services providers for the purpose of identity and eligibility verification.

Powers relating to verification of identity or status

23 Since 6 April 2022, employers and landlords have been able to use Identity Service Providers (IDSPs), also known as Digital Verification Service (DVS) providers, to carry out the digital identity checking element of Right to Work and Right to Rent checks. Completion of the prescribed checks provides the employer, landlord or letting agent with a statutory excuse against the imposition of a civil penalty if found to be employing or renting to someone disqualified from work or renting in the private rented sector as a result of their immigration status. An employer or other relevant person may also be required to carry out prescribed right to work checks in order to comply with the terms of an illegal working compliance order.

24 The use of IDSPs is currently limited to checks of valid British or Irish passports (or Irish passport card), noting the holders of these are not in scope to use the Home Office online checking services.

25 This system of right to work and right to rent checks was introduced under existing powers in the Immigration, Asylum and Nationality Act 2006, the Immigration Act 2014 and the Immigration Act 2016.

26 The amendment will enable the Home Office to legislate to require employers and landlords who carry out right to work and right to rent checks using Identity Document Validation Technology (IDVT) to use the services of DVS Providers who are noted in the register established under Part 2 of the Bill as complying with designated supplementary rules concerning these checks.

27 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.

National Underground Asset Register

28 There is estimated to be around 4 million kilometres of buried pipes and cables in the UK, and a hole is dug every 7 seconds to install, fix, maintain or repair these assets that are critical in keeping the water running, gas and electricity flowing and telecommunications lines connected. Approximately 1 in every 65 holes dug results in an accidental asset strike (c. 60,000 a year), causing around £2.4 billion worth of economic cost, putting workers' lives at risk and causing disruption.

29 There are 600+ owners of underground assets (or "apparatus") across the public and private sectors (including energy, water, telecommunications and local and transport authorities) who

hold data about their own apparatus, which they are required by law to share for the purposes of 'safe digging'. However, currently there is no standardised method to do this with multiple organisations having to be contacted for each dig, providing information in varied formats, scales, quality and on different timelines resulting in a complex process for installing, maintaining, operating and repairing buried apparatus.

30 This Bill will streamline the data-sharing process, reduce the risk of potentially lethal utility strikes on apparatus and promote more efficient management and maintenance of underground apparatus, through establishment, on a statutory footing, of the National Underground Asset Register ("NUAR"). NUAR is a digital map that seeks to improve both the efficiency and safety of underground work by providing secure access to location data about pipes, cables and other types of apparatus installed in streets.

31 The measures update existing data sharing obligations related to buried apparatus to take advantage of the opportunities provided by the data and technology developments that have happened since the previous legislative measures were made. They simplify and expedite the process by which apparatus data is shared by requiring undertakers to share their data in a prescribed manner through NUAR. This will ensure workers have access to up-to-date, comprehensive and standardised data when they need it, to carry out their work effectively and safely. The updated legislation will also ensure a sustainable ongoing service through introduction of fees on those who benefit from the service, rather than relying on taxpayer funding. The provisions allow for data to be made available for purposes beyond safe digging, where appropriate.

Registers of births and deaths

32 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.

33 This Bill will 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.

34 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.

35 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. It will also provide flexibility in how births and deaths are registered in the future, removing the requirement for face-to-face registration.

Changes to the Data Protection Act 2018, UK General Data Protection Regulation and the Privacy and Electronic Communications Regulations 2003

36 Targeted reforms to the UK's data protection legislation are intended to maintain high standards of protection, whilst facilitating the safe deployment and development of modern technologies, and the responsible use of personal data. These reforms are intended to support economic growth and a modern digital government. Changes include:

- making it clear that research organisations can seek broad consent for areas of scientific research,
- allowing legitimate researchers doing scientific research in commercial settings to make equal use of the provisions by clarifying that commercial research activities can benefit from the special position of research in the data protection framework,
- the creation of a new lawful ground under the UK GDPR of 'recognised legitimate interests',
- clarification of the rules in relation to the purpose limitation principle to address existing uncertainty around re-using personal data, including for public interest purposes; and
- expanding the lawful base for the use of solely automated decision-making to make significant decisions about individuals and clarification around the safeguards that must be in place when organisations are carrying out processing of such nature.

37 The Bill will also modernise the governance structures of the ICO by:

- introducing a chair, non-executive and chief executive roles;
- providing a clearer framework of objectives and duties on which to report to Parliament; and
- introducing new, stronger powers of enforcement.

38 The Bill will update the Privacy and Electronic Communications Regulations 2003 through new provisions on: unsolicited direct marketing communications (e.g. nuisance calls); personal data breach reporting by communications service providers; confidentiality of terminal equipment; ICO's enforcement powers; and sectoral codes of conduct. The Bill clarifies 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.

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

39 Some of the differences between Part 3 of the DPA 2018 (which covers law enforcement processing) and the UK GDPR cause difficulties for competent authorities who process under both regimes depending on whether the processing is for a law enforcement or general purpose respectively.

40 This Bill will make changes to Part 3 DPA 2018 in order to reduce 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 national security. All of these provisions currently exist under the UK GDPR.

41 The Bill will also amend Part 3 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, including reconsideration with meaningful human involvement as soon as reasonably practicable. 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.

42 The Bill will also remove the requirement to record a justification in the logs of consultation and disclosure, which is resource intensive and holds limited value in maintaining accountability since it is unlikely that someone accessing the log for an improper purpose would enter an honest justification. The other safeguards, such as the requirement to record the time and date of consultation or disclosure, will remain in the legislation.

43 The current situation where law enforcement agencies 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 will 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 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.

Information standards for health and social care

44 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.

45 This Bill would improve people's lives and life chances, by enabling more and better digital health and care services and, supporting appropriate data-sharing across the wider health and adult social care sector.

Smart meter communication services

46 The Smart Metering Implementation Programme is a Government Major Project Portfolio (GMPP) Programme that is estimated to deliver a net benefit to Great Britain of £6 billion[1]. The Government believes that its successful implementation is key for delivering energy bill reductions, improved customer service and the cost-effective delivery of net zero, by enabling the integration of renewables and emerging technologies such as heat pumps and electric vehicles.

47 Central to the operation of smart metering is the activity of communicating to and from smart metering systems. The GB-wide smart meter communication service is provided by a single licensed entity, regulated by the Gas and Electricity Markets Authority (GEMA). Smart DCC Ltd was awarded the smart meter communication licence under section 6 of the Electricity Act 1989 and section 7AB of the Gas Act 1986 in September 2013 following an open competition and the licence term is coming to an end.

48 This Bill will provide the Authority with flexibility to determine the best process to follow in appointing the successor smart meter communication licensee. This intends to ensure that the Authority is able to appoint a successor in a timely and efficient way that is in the best interest of energy consumers.

Information to improve public service delivery

49 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. With the intention of facilitating 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.

50 The aim of extending the powers is to enable businesses to access government services and support more easily, giving them easier access to information, guidance and business support services.

Retention of information by providers of internet services

51 The Online Safety Act 2023 ("OSA") allows OFCOM to issue information notices to social media companies and other online services. These notices require recipients to provide certain data to OFCOM for the purposes of responding to an information request from the coroner or Procurator Fiscal in Scotland, or for preparing a report under s.163 of the OSA.

52 This Bill expands on this. When a coroner or Procurator Fiscal suspects a child may have taken their own life, they can notify OFCOM. OFCOM must then issue information notices ordering providers of specified regulated services to preserve data on that child's use of those services for a period of time where that information may be needed to respond to an information notice issued under s.101 or to produce a report under section 163 of the OSA.

53 This Bill also enables OFCOM to issue information notices requiring any other relevant person (as defined in the OSA) to preserve data relating to the use of specified regulated services by that child where that information may be needed to respond to an information notice issued under s.101 or to produce a report under s.163 of the OSA.

---

[1] Smart meter roll-out: cost-benefit analysis 2019 (September 2019)

54 The data preservation measure ensures that information on the child's social media and internet use remains available for the investigation by the coroner or Procurator Fiscal or should OFCOM need it in order to respond to a request from a coroner or Procurator Fiscal or to produce a report under s.163 of the OSA. It prevents the data being deleted through routine processes while an investigation is active.

55 The enforcement powers and penalties in the OSA for not complying with OFCOM information notices will apply to the new preservation measure, although the Bill creates a limited number of new criminal offences tailored to this information notice process.

Information for research about online safety matters

56 The provisions in this Bill allow the Secretary of State to make regulations that create a new framework that would permit researchers access to information held by certain providers of internet services, for the purposes of research into online safety matters. OFCOM are currently preparing a report that will provide significant evidence on the issue of access to online safety data for researchers. This report will provide a solid evidence base to inform the design of the access framework, and the Secretary of State will be under a duty to consult with OFCOM and other appropriate bodies before making regulations.

Retention of biometric data

57 Sections 18 to 18E of the Counter-Terrorism Act 2008 (CTA) set out the framework for the retention of biometrics (fingerprints and DNA profiles) for national security purposes. The CTA sets out a standard retention period for biometrics processed under this framework. Biometrics can be held for up to three years from the point at which the biometrics were taken, unless the individual has a prior UK conviction for a recordable offence, or, in cases where the police do not know the identity of the individual to whom the biometrics relate, under which circumstances they can be retained indefinitely. The CTA also includes the power for the police to submit National Security Determinations (NSDs) in cases where the individual does not have a conviction, but the police consider that it is both necessary and proportionate for the purposes of national security to retain the biometrics. NSDs require approval by a Chief Officer, and are reviewed by the independent Biometrics and Surveillance Camera Commissioner. An NSD can be approved for up to five years, and can be renewed.

58 Where the police receive biometrics of national security interest from overseas partners, they process these under the CTA framework (the biometrics processed under the CTA can be referred to as 'section 18 material'). As the volumes of these international biometrics have increased over time, particularly those biometrics received from INTERPOL, the existing retention rules in the CTA have increasingly presented operational challenges for the police. Specifically, an NSD requires a substantial amount of information in order to present a sufficient national security case which can justify the necessity and proportionality of retaining the biometrics for a longer period. This level of information is often not available for biometrics received from overseas, and the volumes involved mean that this is becoming unsustainable for the police to process such a high number of NSDs. The changes in this Bill will mitigate these issues by ensuring that biometrics of national security interest received from overseas partners (or that relate to persons who have overseas convictions) will be able to be retained by the police, where they may have otherwise needed to be destroyed, whilst ensuring retention minimises the intrusion on individual rights.

Trust services

59 Trust services such as electronic signatures, seals, and timestamps increase confidence in the use of electronic transactions through mechanisms such as verifying the identity of individuals and businesses online and confirming the integrity of electronic data e.g. documents. Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (incorporated in UK law at the end of the EU Transition Period under section 3 of the EUWA 2018) as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019/89, provides the legal framework for the use of trust services in the UK and the recognition of equivalent EU trust services. The ICO is the supervisory body for qualified trust service providers and can carry out audits, grant qualified' status, and take enforcement action.

60 The measures in the Bill are aimed at ensuring the effective functioning of the UK regime and making it work for future arrangements. This is being done to make sure that it is ready to support a future demand for secure and trusted electronic transactions in the UK.

61 Additional measures in the Bill will prepare the UK to fully participate in the global digital economy by providing the legal basis for mutual recognition agreements on trust services with other countries. As the digital economy grows globally, there is increasing interest in the interoperability of trust services across borders. This Bill will support interoperability which facilitates international business, reduces trade friction, lowers costs, and enhances confidence and security.

Consultations

Access to customer data and business data

62 In 2018, the previous government consulted 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 financial sectors, as well as charities and academia.

63 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.

64 The previous 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.

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

Digital identity and attributes consultation

66 In July 2021 the previous 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.

67 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.

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

National Underground Asset Register

69 In 2022, the previous government consulted on the future of the National Underground Asset Register to elicit views on current practices in relation to how data is shared and accessed, the potential need for legislative reform to ensure data in the register is complete and up-to-date, and the running of the service once fully operational. The consultation also elicited views on the future funding model.

70 In total 164 responses were received representing a range of interested groups, including local authorities, utility companies, surveyors, regulators and members of the public. The findings included the view that legislative reform would be needed to ensure workers are able to access complete data through NUAR; a preference for the NUAR database to continue to be controlled by government due to commercial and security risk; and calls to explore opportunities for NUAR data to be accessed for other use cases or by other user groups. There was no consensus on who should fund NUAR in the operational phase but general agreement that those who benefit from the service should contribute. In response, the previous government committed to:

a. Developing a charging framework that takes into account the comments raised by respondents

b. Continuing to explore potential legislative reform

c. Considering opportunities for the wider market to enhance the NUAR service

71 The previous government's response to the consultation was published on 24 October 2022.

National Data Strategy and ‘Data: A New Direction’ consultation

72 At the end of 2020, the previous government launched its National Data Strategy, and in September 2021 that government launched the “Data: a new direction” consultation.

73 This consultation closed in November 2021 having received close to 3000 responses. These were received from individuals, businesses, and other organisations including global think tanks, non-profit organisations, research institutes and trade bodies.

74 The previous government's response to the consultation was published on 17 June 2022.

Legal background

Access to customer data and business data

75 Part 1 contains 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, 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 to publish or provide customers or other parties with contextual information relating to the goods, services or digital content provided by the supplier (business data). Part 1 is intended to facilitate the secure sharing of data with authorised third parties, at the customer's request and in "real time", and provision of data in this way is referred to as "smart data".

76 The Part 1 powers are intended to be used to facilitate the long-term continuation of open banking and extend its benefits in an open finance scheme, both of which the Government committed to support in its manifesto. They also largely reflect clauses in Part 3 of the Data Protection and Digital Information Bill of the 2022-3 and 2023-4 sessions the objectives of which, further to a consultation in 2019, was to enact powers to introduce smart data schemes across the economy.

77 The powers, where they are exercised, are intended 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.

78 These powers will replace the regulation-making powers in sections 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.

79 The Government is of the view that 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.

80 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 banking providers in the UK to open up data relating to personal and business current accounts. The largest banking providers were required to set up the Open Banking Implementation Entity to oversee the scheme and to develop standards for data sharing interfaces to be used in the scheme. 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, and over 10 million customers now use it.

81 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 2000 (“FSMA 2000")) for pensions dashboards, an electronic communications service which allows individuals to access information about their pensions in one place.

Digital Verification Services

82 The digital verification service market is a nascent one, and although there exist various disparate laws, standards and guidance which persons providing such services should follow, this Bill establishes a legislative structure which includes rules which such persons must comply with if they wish to be registered on a government register, use a Trust Mark and access an information gateway through which public authorities will be permitted to share information.

83 This legislative structure will make it much easier for an individual who wants to use digital verification services to recognise trusted digital identity providers within the digital identity market.

Powers relating to verification of identity or status

84 The Home Office has powers to prescribe right to work and right to rent checks for employers and landlords to follow, in order to obtain a statutory excuse (defence) against a civil penalty for employing or renting to a disqualified person. A disqualified person is a person who is prevented from working or renting due to their immigration status. A person specified in an illegal working compliance order may also be required to carry out right to work checks in order to comply with the terms of an illegal working compliance order.

85 This Bill amends powers in the Immigration, Asylum and Nationality Act 2006, the Immigration Act 2014 and the Immigration Act 2016 so that the Home Office can require by way of orders/regulations employers, landlords and persons specified in an illegal working compliance order, where they choose to carry out certain digital checks in place of manual checks, to use the services of organisations registered as complying with designated supplementary rules concerning the provision of these services.

National Underground Asset Register

86 The Bill sets out a new legal framework which will put the National Underground Asset Register (“NUAR”) on a statutory footing by imposing a new duty on the Secretary of State to keep a register, i.e., NUAR, and make the information in NUAR available to other persons. The Bill achieves this by building upon and modernising existing provisions made in the New Roads and Street Works Act 1991 (“the 1991 Act”) for England and Wales, and in the Street Works (Northern Ireland) Order 1995 (“the 1995 Order”).

Registers of births and deaths

87 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.

Data Protection

88 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.

89 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").

90 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 (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.

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

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

93 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.

94 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 DPA 2018;
- processing by "competent authorities" (as defined in section 30 & schedule 7 DPA 2018) for law enforcement purposes - governed by Part 3 DPA 2018; and
- processing by the UK intelligence services - governed by Part 4 DPA 2018.

95 Part 5 DPA 2018 sets matters concerning the constitution, functions, powers and duties of the Information Commissioner. Part 6 sets out enforcement procedures.

Privacy and Electronic Communications Regulations

96 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.

97 The Data (Use and Access) Bill makes various amendments to these existing sources of data protection law.

Information standards for health and social care

98 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.

99 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 or 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 (unless that requirement is waived), except that the Secretary of State is required only to have regard to an information standard published by NHS England.

Smart meter communication services

100 The provisions insert new sections into the Energy Act 2008 and make consequential amendments to the Electricity Act 1989 and Gas Act 1986 in order to provide the Authority with the flexibility to determine whether to appoint the smart meter communication licensee via a competitive or non-competitive process.

Information to improve public service delivery

101 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 125 of this Bill amends section 35 to extend these data sharing powers to support the delivery of public services which benefit businesses, or "undertakings".

102 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.

103 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.

Retention of information by providers of internet services

104 Section 101 of the Online Safety Act 2023 ("OSA") created a new power for OFCOM to issue information notices to relevant persons (as defined by s.100(5)(a)-(e) requiring them to provide information to OFCOM for the purposes set out in s.101(1)).

105 The provision in the Bill builds on this, by creating a requirement for OFCOM, when notified of a child death by the Coroner (or Procurator Fiscal in Scotland), to issue an information notice to providers of specified kinds of regulated service requiring them to retain certain information relating to the use of the service by the deceased child for a specified period.

106 It also gives OFCOM the power, where relevant, to issue such information notices to any other relevant person (as defined in s.101 OSA) requiring retention of information relating to a child's use of specific kinds of regulated service[2].

107 The provision will help ensure that in those cases caught, should OFCOM, the Coroner or the Procurator Fiscal require the information it has not been deleted through routine processes or otherwise.

108 The provision also provides for the enforcement powers relating to information notices issued under s.101 of the OSA to apply to the new information notices under this provision, and creates additional criminal offences tailored to this provision.

Information for research about online safety matters

109 The Online Safety Act 2023 creates a new regulatory regime, overseen by OFCOM, imposing various duties on the providers of certain internet services, to include 'user-to-user services' and 'search services'.

110 Section 162 OSA requires OFCOM to prepare a report, which must be published by July 2025, that will describe how, and to what extent, persons carrying out independent research into online safety matters are currently able to obtain information from providers of regulated services to inform their research. It will also explore the legal and other issues which currently constrain the sharing of information with researchers and will assess the extent to which greater access to information for such purposes might be achieved.

Trust services

111 Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (incorporated in UK law at the end of the EU Transition Period under section 3 of the EUWA 2018) as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019/89, provides the legal framework for the use of trust services in the UK and the recognition of equivalent EU trust services.

112 There are also some specific provisions on its effect, supervision and enforcement in the UK. These requirements were transposed in the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (EITSET Regulations), which designate the Information Commissioner (the "IC") as the UK's supervisory body and sets out an enforcement regime. The EITSET Regulations were amended by the DPA 2018 to reflect changes in the IC's investigative powers.

113 The provisions in the Bill aim to support the effective functioning and ongoing development of the UK trust services market.

[2] This is intended to capture, for example, information held by ex-providers.

Territorial extent and application

114 Clause 135 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.

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

Access to customer data and business data

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

Digital Verification Services

117 The territorial extent of these provisions is UK wide.

Powers relating to verification of identity or status

118 The territorial extent of clause 55 is UK-wide. Whilst the Right to Work Scheme operates UK-wide, the power to issue a civil penalty for a breach of the Right to Rent Scheme is currently in force in England only. Orders prescribing requirements under Chapter 1 of Part 3 of the Immigration Act 2014 will only have a practical effect in England, until such time as the Right to Rent Scheme is rolled out to other areas of the UK.

National Underground Asset Register

119 Collectively, the clauses relating to NUAR make equivalent provision across England, Wales and Northern Ireland. To deliver this, specific changes need to be made to legislation extending to England and Wales, and equivalent legislation extending to Northern Ireland. Clauses 56, 57(1) to (9), 60(1) and Schedule 1 therefore extend to England and Wales, whilst clauses 58, 59, 60(2) and Schedule 2 extend to Northern Ireland.

120 The NUAR provisions in the Bill extend to England, Wales and Northern Ireland. The Bill does not make provisions for Scotland as Scotland already benefits from a system of this kind through the Scottish Community Apparatus Data Vault (VAULT), implemented by the Office of the Scottish Road Works Commissioner, which makes information about all underground pipes and cables in Scotland available from one centralised location.

Registers of Births and Deaths

121 The clauses which amend the Births and Deaths Registration Act 1953 and the Registration Service Act 1953, relating to the form in which registers are to be kept and the provision of equipment and facilities by local authorities, extend and apply to England and Wales only.

122 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 some of the provisions amended extend to Scotland and Northern Ireland.

Data protection

123 The Bill's amendments to the UK GDPR and DPA 2018 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

124 Changes to the Privacy and Electronic Communications (EC Directive) Regulations 2003 in Part 4 extend to the whole of the UK.

Information standards for health and social care

125 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.

Smart meter communication services

126 The territorial extent and application of most of these provisions is Great Britain.

Information to improve public service delivery

127 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).

128 Currently, under section 44 and section 45 of the DEA 2017, the "appropriate national authority" in relation to the information-sharing powers under section 35 (which is either the Secretary of State for Science, Innovation and Technology, 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).

129 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".

Retention of information by providers of internet services

130 This provision extends and applies to the whole of the UK. As this provision amends the Online Safety Act 2023, which applies to providers of regulated services (as defined in s.4(4) of that Act) based outside the UK, this provision applies extraterritorially in such cases also[3].

Information for research about online safety matters

131 These provisions extend and apply to the whole of the UK and will have extra-territorial application to the extent they apply to regulated services (as defined in s.4(2) and (4) of the Online Safety Act 2023) which are based outside the UK.

Retention of biometric data

132 These provisions extend UK-wide but apply only to the processing of biometric material by a law enforcement authority under the law of England and Wales and Northern Ireland (a different regime applies in Scotland).

Trust services

133 The territorial extent of these provisions is UK wide.

[3] See sections 204 and 205 of the Online Safety Act 2023.

Commentary on provisions of Bill

Part 1: Access to Customer Data and Business Data

Introductory

Clause 1: Customer data and business data

134 Clause 1 defines key terms and concepts for the regulation-making powers in Part1.

135 Subsection (2) defines the terms "business data", "customer data", "data holder", "data regulations" and "trader".

136 "Business data" is general information about goods, services and digital content supplied or provided by a trader; their supply or provision, which may include information about their availability (for example, in a communications context, information about a supplier's broadband coverage); their price (which enables price comparisons against competitors) and other terms of supply; information about feedback; and information about the use, performance or quality of the goods, services or digital content in question. Business data may also include information about the provision of business data under the regulations.

137 "Customer data" is information specific to a customer of a trader. Without limitation, customer data includes information about the goods, services or digital content supplied or provided by a trader to that customer or to another person (recipient) at the customer's request. This might encompass information on the prices that customer has paid or is paying (which could aid personalised price comparisons), information about other terms relating to the supply or provision of the goods, services or digital content in question, information on the use of the goods, services or digital content such as usage patterns, and information about the performance or quality of the goods, services or digital content. In the context of the provision of banking services, customer data could include the customer's balance and transaction history. Customer data may also include information about the provision of customer data to a person under the regulations.

138 A "data holder" is a trader (paragraph (a) of the definition) but also covers a person who, in the course of business, processes the data (paragraph (b)). Regulations under clauses 2 and 4 impose obligations on data holders, and paragraph (b) of the definition ensures that those obligations may apply to persons who hold data on the trader's behalf.

139 "Data regulations" are regulations relating to customer data and business data under clauses 2 and 4 (and may be read to include regulations to which clause 23 (other data provision) applies: see clause 23(3)).

140 Aside from the "data regulations", Part 1 contains other, ancillary, regulation-making powers in clauses 8 (enforcement), 11 (fees), 12 (levy), 14 (FCA and financial services interfaces), 16 (FCA and financial services interfaces: penalties and levies), 17 (the FCA and co-ordination with other regulators), 18 (liability in damages) and 19 (duty to review regulations). References in these notes to "Part 1 regulations" are to regulations under any or all powers in Part 1 whether or not they are data regulations.

141 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.

142 The definitions of "business data", "customer data", and "trader" are framed by reference to the supply or provision of goods, services and digital content. The application of Part 1 to "goods", "services", "digital content" reflects the approach of Part 1 (Consumer contracts for goods, digital content and services) of the Consumer Rights Act 2015. However, "digital content" and "goods" are defined for the purpose of Part 1 in clause 25(1). Unlike the 2015 Act, "goods" includes water, gas and electricity without restriction as to how or in what quantity they are supplied.

143 Subsections (3)-(5) describe when, and in relation to what, a person is a customer of a trader for the purposes of Part 1.

144 Subsection (3) ensures that a person (C) may be a customer of a trader (T) not only where C purchases goods, services or digital content ("goods etc.") from T, but where C is supplied goods etc. purchased by another person and where C receives goods etc. free of charge.

145 Subsection (4) ensures that a person may be treated as a customer in relation to the purchase, supply, provision or receipt of goods etc. before this clause comes into force.

146 Subsection (5) confirms that a person is considered a customer from the point of entering into agreement to purchase the goods etc. from T, and not just when those things are provided to the customer or recipient.

147 Customers are intended to include, but are not restricted to, consumers. Regulations may therefore apply to customers acting for purposes relating to a course of business including customers which are corporate entities. The breadth of the concept of customer reflects that business customers – particularly small businesses – may suffer from similar disadvantages relating to access to data as consumers, and it may not always be practicable for regulations to distinguish between different kinds of customer. Pursuant to clause 21(1)(a) and (b), data regulations may be made to apply only to certain categories of customer.

148 Subsection (6) provides that references to the provision or receipt of data should be read as including access to data by that person or other persons. This reflects that, in practice, data might not be transferred from one person to another; rather, it may be the case that the person is granted access to data which is, and remains, held by the data holder.

Data regulations

Clause 2: Power to make provision in connection with customer data

149 Clause 2 provides the principal regulation-making power in relation to customer data.

150 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 (paragraph (a)) or to a person of a specified description who is authorised by the customer to receive the data (an "authorised person"), at the request of the customer or the authorised person (paragraph (b)).

151 It is intended that data regulations will most likely require the provision of customer data to an authorised person (under paragraph (b)) rather than directly to the customer (under paragraph (a)) since the authorised person will be best able to make use of the data on the customer's behalf (for instance, in the provision of innovative services such as account management services via a visual dashboard of accounts, displayed on a smartphone application). However, the regulation-making powers have been kept broad to allow regulations to provide for direct provision of data to customers in the future.

152 Subsection (2) defines, in relation to customer data, a "third party recipient". A third party recipient is a person of a description specified (see further "specified" in clause 25(1)) under subsection (1)(b) who a customer is able to authorise. The concept of a third party recipient is distinct from that of an authorised person: this is because regulations may impose requirements (such to have appropriate IT systems or to pay fees or a levy) on persons of the specified description. That may be the case where a person is "accredited" as a third party recipient by a decision-maker under clause 6, but might not necessarily be authorised by a customer at any particular time. Clause 3(2)(b) and (c) illustrates possible means by which the regulations may restrict the persons customers may authorise to act on their behalf.

153 Subsection (3)(a) provides for the making of regulations which enable or require data holders to produce, collect or retain customer data or arrange for that to be done. The purpose of this power is to ensure that data holders have specific data to hand which will ensure that smart data schemes can operate consistently and effectively. This subsection, as Part 1 more generally, is to be read in accordance with clause 20(2): it would not, therefore, override a data subject's right to data erasure under Article 17 of the UK GDPR.

154 Subsection (3)(b) provides for the making of regulations which enable or require data holders to make changes to customer data if requested by the customer or an authorised person. 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 customer data where a customer is not an individual.

155 Subsection (4) enables the making of regulations which provide for an authorised person to be able take, on the customer's behalf, action that the customer could take 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 (for instance, to make a payment from the customer's account) or transact with the trader (for instance, to negotiate an improved deal) on the customer's behalf.

156 Subsection (5) requires that in deciding whether to make regulations under clause 2, the Secretary of State or the Treasury must (among other things) consider the likely effect of the regulations on customers, data holders, small and micro businesses, and on innovation in the supply of goods and products and competition. The concepts of small and micro-business are defined in clause 25(1) by reference to the Small Business, Enterprise and Employment Act 2015.

Clause 3: Customer data: supplementary

157 Clause 3 illustrates provisions that data regulations under clause 2 may, among other things, contain. Data regulations do not have to contain all of these provisions, neither are they limited to them.

158 Subsection (2) envisages that regulations may include: provisions about the procedure by which customers authorise a person to access their data or otherwise act on their behalf (paragraph (a)); provisions restricting the persons that a customer may authorise to those complying with conditions specified by or under the regulations (paragraph (b)); and provisions for a person (a decision-maker) to decide whether a person satisfies those conditions (paragraph (c)) . Paragraph (c) envisages the possibility of a system of accreditation for third party recipients: if so, clause 6 (decision-makers) will apply and that clause contains further provisions and requirements about decision-makers.

159 Subsection (3) envisages provisions about the making of requests relating to customer data: the regulations may, for instance, impose requirements as to how requests may be made. Subsection (3) also envisages that regulations may provide circumstances in which a data holder may or must refuse to act on a request: such circumstances might, for instance, include unfounded or excessive requests.

160 Subsection (4) envisages provisions about how customer data is to be provided and action is to be taken on the customer's behalf in accordance with regulations under clause 2(4).

161 Subsection (4)(a) envisages that customer data may be provided on one or more occasions, for a specified period (e.g., continuously available for a set amount of time) or at specified intervals.

162 Subsection (4)(b) envisages requirements for the use of specified facilities or services, including electronic communications services or application programming interfaces (see clause 25(1)) (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 API standards that were designed by a separate implementation body, to ensure the timely sharing of customer data.

163 Subsection (4)(c) envisages requirements on data holders and third party recipients to comply with specified standards, or participate in specified arrangements, relating to, or to the use of, those facilities or services. For example, data holders and third party recipients 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.

164 Subsection (4)(d) envisages requirements on data holders and third party recipients to provide for, or arrange, specified assistance in relation to establishing, maintaining or managing those facilities or services. Subsection (11) provides that assistance may include actual or contingent financial assistance and gives examples of such assistance.

165 Subsection (4)(e) envisages provisions about interface bodies. These are dealt with in clause 7 (interface bodies). Interface bodies may undertake the tasks in subsection (1) of that clause.

166 Subsection (5) envisages provisions requiring or enabling data holders and third party recipients to produce, collect, or retain records of their provision or (as the case may be) receipt of customer data.

167 Subsection (6) envisages that a person who processes customer data may be required to assist a trader in complying with the regulations.

168 Subsection (7) envisages requirements on third party recipients relating to the processing of customer data by them: paragraphs (a) to (d) reflect paragraphs (b) to (e) of subsection (4) with subsection (11) applying in relation to the specified assistance referred to paragraph (c). Paragraph (e) envisages the imposition of requirements in relation to any further disclosure of that data, including on "downstream" recipients.

169 Subsection (8) envisages provisions enabling or requiring a data holder or third party recipient to publish specified information about rights and obligations under the regulations. Such provisions may be important, for instance, to require traders to draw customers' attention to their rights and how they may be exercised.

170 Subsection (9) envisages provision about complaints which may include a requirement for data holders and third party recipients to implement complaints procedures (decision-makers may also be required to implement such procedures under clause 6(7)).

171 Subsection (10) envisages provision 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 about review of decisions and for appeals to a court or tribunal. By way of example, a person determining a dispute may be a recognised ombudsman in a given sector, or simply an alternative dispute resolution (ADR) provider.

172 Subsection (11) is explained in the context of subsections (4)(d) and (7)(c).

Clause 4: Power to make provision in connection with business data

173 Clause 4 provides the principal regulation-making power in relation to business data. This regulation-making power may be used in conjunction with clause 2 or on its own.

174 Subsection (1) enables the Secretary of State or the Treasury to make regulations requiring data holders to publish business data and/or provide business data to the customer (paragraph (a)) or to another person of a specified description (paragraph (b)).

175 As business data does not directly relate to a particular customer, there are two important differences as compared with the equivalent regulation-making power for customer data in clause 2(1). First, regulations under subsection (1) of this clause may require publication of data: this is because, depending on the smart data scheme in question, it might be efficient to publish data in accordance with such arrangements as the regulations may prescribe. Second, if the regulations take the approach of requiring provision of data to a person of a specified description, that person does not require the authorisation of a customer.

176 Subsection (2) defines, in relation to business data, a "third party recipient" for the purpose of Part 1: a third party recipient is a person of a description specified under subsection (1)(b). In practice, the same person may be a third party recipient under clauses 2(1) and 4(1) for both customer data and business data.

177 Subsection (3) provides for the making of regulations which enable or require data holders to produce, collect or retain business data or arrange for that to be done. As with clause 2(3)(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.

178 Subsection (4) enables the making of regulations which require a public authority (see clause 25(1)), or a person appointed by a public authority, which is a third-party recipient of business data to publish or provide that data. This is to enable a model in which business data is provided to, and then published or disclosed onwards by, a public authority or a person acting on its behalf. To enable this model to function, paragraph (b) allows the regulations to impose requirements (except a requirement to pay the levy under clause 12) on the public authority or its appointee as if it were a data holder and paragraph (c) allows the regulations to treat a person ultimately receiving the data as a third party recipient.

179 Subsection (5) mirrors clause 2(5) and requires that, in deciding whether to make regulations relating to business data, the Secretary of State or the Treasury must (among other things) consider the likely 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 5: Business data: supplementary

180 Clause 5 illustrates provisions that data regulations under clause 4 may, among other things, contain. This clause largely mirrors clause 3 (provision of customer data: supplementary) and, as with that clause, data regulations do not have to contain all of the provisions envisaged by clause 5 and neither are they limited to them.

181 Subsection (2) envisages that regulations may require business data to be provided on request. The regulations may provide for requests for business data to be made by a customer, third party recipient or by other persons. If the regulations provide for the provision of data on request then, as with clause 3(3) in relation to customer data, the regulations may contain provision about those requests including circumstances in which a data holder may or must refuse to act on a request.

182 Subsection (3) envisages provisions restricting provision of business data to customers or to third party recipients who are approved to receive it. If so, as with clause 3(2), the restriction may be achieved by conditions specified by or under the regulations (paragraph (a)) and the regulations may provide for a specified person (a decision-maker) to decide whether a person satisfies those conditions. Clause 6 (decision-makers) contains further requirements about decision-makers, should the regulations make such provision.

183 Subsection (4) envisages provisions about how business data is to be published or provided, reflecting, in relation to provision of business data, clause 3(4).

184 Subsection (5) envisages provisions requiring or enabling data holders and/or third party recipients to produce, collect, or retain records of their provision or (as the case may be) receipt of business data, reflecting clause 3(5).

185 Subsection (6) envisages that a person who processes business data may be required to assist a trader in complying with the regulations, reflecting clause 3(6).

186 Subsection (7) envisages requirements on third party recipients and on "downstream" recipients relating to the processing of business data, reflecting clause 3(7).

187 Subsection (8) envisages provisions enabling or requiring a data holder or third-party recipient to publish specified information about rights and obligations under the regulations, reflecting clause 3(8).

188 Subsection (9) envisages provision about complaints, which may include a requirement for data holders or third party recipients to implement complaints procedures, reflecting clause 3(9).

189 Subsection (10) envisages provisions for dispute resolution, reflecting clause 3(10).

190 Subsection (11) sets out what is meant by assistance in subsections (4)(d) and (7)(c), reflecting clause 3(11).

Clause 6: Decision-makers

191 Clause 6 outlines provisions relating to decision makers that data regulations may, among other things, provide for. The possible provisions in this clause are non-exhaustive, but, if regulations do provide for a decision-maker, subsection (7) is mandatory.

192 A decision-maker (see subsection (2)) is a person on which the regulations confer the function of deciding whether a person satisfies conditions restricting who customers may authorise to receive customer data or do other things (clause 3(3)(b)) and who may be approved to receive

business data (clause 5(3)(b)). Decision-makers might (if they are a public authority), or might not, be persons who are enforcers under clause 8 (enforcement of data regulations).

193 Clause 6 deals with the conferral of decision-making functions in the context of those provisions. Clause 21(1)(g) allows for the conferral of functions involving the exercise of a discretion in other contexts.

194 Subsection (3) provides that regulations may make provision about the appointment of the decision-maker.

195 Subsection (4) provides that regulations may enable or require decision-makers to suspend or revoke decisions. A revocation or suspension may result in the person concerned ceasing to be able to request or receive data or to act on a customer's behalf. However, it is anticipated that a suspension or revocation might alternatively be used to impose a lesser sanction for instance, through a partial suspension or revocation, one which allows a third party recipient to continue to act in that capacity subject to conditions or additional conditions. In providing for, or requiring, a decision-maker to suspend or revoke its decisions, the regulations may, among other things, make different provisions for different cases and may make consequential, supplementary and incidental provisions (see clause 21(1)).

196 Subsection (5) provides for the conferral of powers on decision-makers to monitor compliance by third party recipients with the conditions under which they are authorised or approved, and these powers are enforceable in the same way as powers conferred on enforcers under clause 8.

197 Subsection (6) clarifies that the monitoring powers referred to in subsection (5) include enabling a decision-maker to require the provision of documents or information, but this is subject to the restrictions on investigatory powers in clause 9.

198 Subsection (7) requires that regulations must make provision about the rights of persons affected by the exercise of decision-makers' functions. These rights may include provisions for review of decisions or rights of appeal to a court or tribunal. This provision is considered a necessary safeguard against a decision to revoke the authorisation or approval of a third party recipient.

199 Subsection (8) provides that regulations may make provision about complaints, including requiring a decision-maker to implement procedures for the handling of complaints.

200 Subsection (9) provides for the regulations to enable or require the publication of specified documents or information relating to the exercise of a decision-maker's functions.

201 Subsection (10) provides for a decision-maker to conduct its investigations through another person and reflects clause 8(11) in relation to enforcers.

202 Subsection (11) provides for the appointment of multiple decision-makers and reflects clause 8(12) in relation to enforcers.

203 Subsection (12) provides for regulations to enable or require a decision-maker to produce guidance about how it intends to exercise its functions under the regulations. Regulations may include requiring the decision maker to publish the guidance and provide copies to specified persons.

Clause 7: Interface bodies

204 Clause 7 is about the provision that regulations under clause 2 and 4 may (among other things) contain about "interface bodies". Such bodies may be required to be established and

maintained in order to provide facilities and services, set standards or make related arrangements for data sharing interfaces. The Open Banking Implementation Entity is an example of an interface body; it has developed API standards to which the largest banking providers are required to adhere under the CMA Order.

205 Subsection (1) outlines the tasks that interface bodies may perform. These are establishing interfaces, which are facilities or services for the sharing of data or the initiation of actions; setting standards or making arrangements relating to, or to the use of, interfaces (which could include interfaces established, managed or maintained by other persons); and maintaining or managing such interfaces, interface standards or interface arrangements.

206 Subsection (2) defines interface bodies with reference to subsection (1).

207 Subsection (3) enables regulations to be made requiring a data holder or a third party recipient to set up an interface body, and to make provision about the type of body to be set up. This is to allow the Secretary of State or the Treasury to require a scheme to have an interface body, and to require participants in the scheme to establish it.

208 Subsection (4) sets out the provisions that regulations may make in relation to an interface body. These include provisions about the composition and governance of the body, things the body must do in relation to interface standards or arrangements, provisions about the body's objectives and how it carries out its functions, requirements in relation to persons required to set up the body including the provision of assistance (see subsection (7)), transparency requirements, and the conferral of monitoring powers on the body. The intention of this is to ensure that interface bodies can be appropriately regulated and that regulations can require industry participants to effectively support such bodies.

209 Subsection (5) confirms that where an interface body is provided with monitoring powers, these include the power to require the provision of documents. The intention of this is to ensure that an interface body can effectively monitor the use of its interface, standards and arrangements. For example, the Open Banking Implementation Entity monitors the implementation, availability and performance of the APIs that it oversees. As with clause 6(6) in relation to decision-makers, these powers are subject to the restrictions on investigatory powers in clause 9.

210 Subsection (6) provides examples of the facilities referred to in subsection (1)

211 Subsection (7) provides that references to "assistance" in subsection (4)(b) and (7)(c) include actual or contingent financial assistance and gives examples of financial assistance.

Enforcement

Clause 8: Enforcement of regulations under this Part

212 Clause 8 enables monitoring compliance with, and enforcement of, Part 1 regulations and requirements imposed under them. This may be conducted by a public authority (see clause 25(1)) which is specified in the regulations and authorised or required to do so (an "enforcer").

213 Subsection (4) deals with the powers of investigation that may be conferred on an enforcer. These include: powers to require provision of information or documents; powers to require an individual to be interviewed; and powers of entry, inspection, search and seizure. The conferral of investigatory powers is subject to the restrictions in clause 9 (restrictions on powers of investigation) as well as any further restrictions in the regulations.

214 Subsections (5) and (7) deal with enforcement powers that may be conferred on an enforcer.

215 Subsection (5)(a) provides for the regulations to enable an enforcer to issue a notice ("compliance notice") requiring compliance with Part 1 regulations, any condition for authorisation or approval of a third party recipient imposed by a decision-maker (see clause 6), or any other requirement imposed in exercise of a power conferred by Part 1 regulations. Subsection (5)(b) enables regulations to make provision for enforcement of compliance notices, as if they were orders of a court or tribunal.

216 Subsection (5)(c) provides that regulations may enable an enforcer to publish a statement that the enforcer considers that a person is not complying with Part 1 regulations, a requirement imposed by a compliance notice or any other requirement imposed in exercise of a power conferred by Part 1 regulations. This allows an enforcer to "name and shame" the person concerned which may, for instance, be useful in persistent or egregious cases of non-compliance.

217 Subsection (7) enables the regulations to allow an enforcer to impose financial penalties in the cases of: provision of false or misleading information; failure to comply with a requirement imposed by Part 1 regulations; failure to comply with a requirement imposed in exercise of a power imposed by Part 1 regulations; failure to comply with a compliance notice. Where either could be imposed, a financial penalty may be imposed additionally or alternatively to the sanctions in subsection (5).

218 Clauses 10 (financial penalties) and 21(3) contain further provisions relating to financial penalties, including procedural and other safeguards that the regulations must contain if they are to provide for the imposition of financial penalties. These are described further in the context of clause 10.

219 Subsection (6) enables the regulations to create offences in cases where a person provides false or misleading information to an enforcer, or an act or omission (including falsification) which prevents an enforcer, interface body or a decision-maker from accessing information, documents, equipment, or other material. The regulations may provide for the offences to be punishable by a fine, which may be either unlimited or not exceeding a specified amount. Pursuant to clause 21(2), the maximum amount must be set out in the regulations or framed by reference to a standard scale, statutory maximum or similar.

220 Subsection (8) enables the regulations to make provision about rights for those (for instance data holders and third party recipients) affected by an enforcer's actions. Such rights may include reviews of the decisions made by an enforcer or appeals to a court or tribunal. In addition, there are specific and mandatory safeguards if the regulations empower an enforcer to issue financial penalties: see clause 10.

221 Subsection (9) enables the regulations to make provision about complaints, including requiring enforcers to implement procedures for the handling of complaints.

222 Subsection (10) enables the regulations to require an enforcer to publish, or provide to a specified person, information relating to its monitoring or 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.

223 Subsection (11) enables an enforcer's powers of investigation to be carried out by another person. This reflects the investigatory powers in relation to consumer law in Schedule 5 to the Consumer Rights Act 2015.

224 Subsection (12) 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.

225 Finally, subsection (13) allows the regulations to enable or require an enforcer to produce, publish and provide guidance about how it intends to exercise its functions.

Clause 9: Restrictions on powers of investigation etc

226 Clause 9 restricts the powers of investigation that may be conferred on enforcers by clause 8. The clause also restricts the monitoring powers that may be conferred on decision-makers (see clause 6(6)) and interface bodies (see clause 7(5)).

227 Subsection (1)(a) ensures that regulations may not authorise entry of an enforcer to a private dwelling without a court-issued warrant.

228 Subsection (1)(b) ensures that regulations may not require a person to give a decision-maker, an interface body or 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 in connection with legal advice relating to obligations, liabilities or rights under Part 1 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 or contemplation of, and for the purpose of, proceedings under or arising out of Part 1 regulations (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)).

229 Subsection (8) prevents an oral or written statement given in response to a request for information from a decision-maker, an interface body 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 10: Financial penalties

230 Clause 10 makes provision in relation to financial penalties and imposes safeguards as to their use.

231 Subsections (2) (except as provided for) and (3) set out requirements with which regulations must include if they confer a power to impose a financial penalty.

232 Subsection (2) provides that, except where clause 16 (the FCA and financial services interfaces: penalties and levies) provides otherwise, a financial penalty may be a penalty of a specified amount, or an amount determined in accordance with the regulations, or an amount not exceeding those amounts. In accordance with clause 21(3) and (4), the specified amount or methodology by which the amount of a penalty is to be determined must be set out in the regulations or by reference to a published index. However, the regulations may require or

enable the enforcer to make decisions, within the framework of that maximum or methodology, about the amount payable in a particular case.

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

234 Under subsection (3)(c), the regulations must require an enforcer to provide a 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").

235 Under subsection (3)(d) and (e), the regulations must require an enforcer to provide that person 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.

236 Under subsection (3)(f), the regulations must require that, if the enforcer then decides to impose a financial penalty, the enforcer must issue that person with a notice in writing (final notice) imposing that penalty.

237 Subsection (3)(g) to (h) 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).

238 Subsection (4) provides that regulations may:

- require or enable an enforcer to provides copies of the guidance to which subsection (3)(a) and (b) to specified persons (paragraph (a));
- enable a notice of intent or final notice to be withdrawn or amended, for example if the circumstances change (paragraph (b));
- set out circumstances under which the enforcer is required to withdraw a final notice (paragraph (c));
- in the case of a late payment, increase a financial penalty by up to a specific amount or an amount determined in accordance with the regulations (paragraph (d)) but this provision is subject to clause 21(3) and (4);
- make provision as to how financial penalties are recoverable (paragraph (e)).

Fees etc and financial assistance

Clause 11: Fees

239 Subsection (1)(a) of clause 11 provides for regulations to allow persons listed in subsection (2), or those acting on their behalf, to require the payment of fees for the purpose of meeting expenses described in subsection (3). Subsection (1)(b) enables regulations to make provision as to what must or may be done with the monies.

240 Subsection (2) lists the persons who the regulations may enable to charge fees.

241 Subsection (2)(a) allows regulations to enable fee charging by data holders. It is intended that, unless the regulations provide otherwise, a data holder's provision of data and its

performance of other obligations should be free to customers and third party recipients. Regulations might, for instance, allow data holders to charges fees in the case of excessive requests for data.

242 Subsections (2)(b)-(e) allows regulations to enable fee charging by decision-makers, interface bodies, enforcers and any other persons carrying out functions imposed or conferred by or under Part 1 regulations.

243 The expenses described in subsection (3), for which regulations may enable fees to be charged under subsection (1)(a), are expenses incurred, or to be incurred, by the persons listed in subsection (2), or by persons acting on their behalf, in the conduct of functions imposed or conferred on them by or under Part 1 regulations.

244 Clause 11 does not deal with, or restrict, the charging of fees by third party recipients: the basis of the arrangements between third party recipients and customers is a commercial matter for them to determine.

245 Subsection (4)(a) limits the persons who may be charged fees. That subsection only permits regulations to provide for payment of fees by persons that appear to the Secretary of State or the Treasury to be capable of being directly affected by the performance of duties, or exercise of powers, under Part 1 regulations. This would include data holders, customers who exercise any rights granted to them under data regulations or by whom a third party recipient is authorised to act, and third party recipients.

246 Subsection (4)(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 the costs incurred in a specific case, in the interests of the efficiency and effectiveness of a smart data scheme.

247 Subsection (5) requires that, except where clause 15 (the FCA and financial services interfaces: supplementary) provides otherwise, a fee must be of a specified amount, an amount determined in accordance with the regulations, or an amount not exceeding those amounts. In accordance with clause 21(3) and (4), the specified amount or methodology by which the fee is to be determined must be set out on the face of the regulations or by reference to a published index. However, the regulations may require or enable a person to make decisions, within the framework of the maximum or methodology, about the amount of fee payable in a particular case.

248 Subsection (6) 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. This is subject to clause 21(3) and (4).

249 Subsection (7) provides that where regulations give a person a discretion to determine the amount of the fee, the regulations must require that person to publish information about the amount and how it is determined.

250 Subsection (8) 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 12: Levy

251 Subsections (1)(a) of clause 12 enables regulations to impose, or (subject to subsection (5)) provide for a specified public authority to impose, a levy on data holders or third party

recipients to meet the expenses described in subsection (2). Subsection (1)(b) enables the regulations to make provision as to what must or may be done with the monies.

252 The expenses described in subsection (2) are expenses incurred, or to be incurred, by a person listed in subsection (3), or a person acting on their behalf, in the conduct of functions imposed or conferred on them by or under Part 1 regulations.

253 The persons listed in subsection (3) are decision-makers, interface bodies, enforcers and public authorities on which requirements are imposed by regulations under clause 4(4).

254 The purpose of the levy is to meet all or part of the costs incurred by those persons so that the expenses of a smart data scheme may be met by the relevant sector without incurring a cost to the taxpayer.

255 Subsection (4) limits the persons on whom the levy may be imposed. That subsection only permits a levy to be imposed on data holders or third party recipients that appear to the Secretary of State or the Treasury to be capable of being directly affected by the exercise of the functions of persons listed in subsection (3).

256 Subsection (5) ensures that, where regulations provide for a levy to be imposed by a public authority, the regulations must specify how the rate of a levy and the period in respect of which it is payable are to be determined. The regulations must also require the public authority to publish information about that rate and period and how they are determined.

257 Subsection (6) 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 13: Financial assistance

258 Subsection (1) of clause 13 provides statutory authority for the Secretary of State or the Treasury to give financial assistance to a person for the purpose of meeting any expenses incurred by that person in performing duties or exercising powers imposed or conferred by or under Part 1 regulations and in exercising connected functions.

259 Subsections (2) and (3) stipulate that financial assistance cannot be provided to data holders, customers, or third party recipients (other than a third party recipient that is a public authority which is subject to requirements imposed by regulations under clause 4(4)), or persons acting on their behalf.

260 Under subsection (4), the assistance may be given on terms and conditions that the Secretary of State or the Treasury deem appropriate.

261 Subsection (5) 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.

262 It is intended that smart data schemes will be "self-financing" (through the fees and levies provided for by clauses 11 and 12) but it is deemed appropriate for there to be a statutory spending authority as a "backstop" should that be necessary.

Financial Services Sector

Clause 14: The FCA and financial services interfaces

263 Clause 14 enables the Treasury to make regulations to confer powers on the Financial Conduct Authority ("FCA") to impose requirements, via rules, on interface bodies used by the financial services sector and on persons participating in, or using the facilities and services provided by, such bodies. This is to allow the FCA to regulate financial services smart data schemes and interface bodies in a manner broadly consistent with its regulation of the wider financial services sector (although with some differences to reflect the specific nature of such bodies and schemes). Direct regulatory oversight of financial services interface bodies is also necessary to allow financial services smart data schemes to operate consistently with the arrangements for Open Banking that have been in place to date under the CMA Order.

264 Subsection (1) permits the Treasury to make regulations to enable or require the FCA to make rules about interfaces used in relation to customer data and business data in financial services. Subsections (1)(a) provides that rules may require financial services providers to use a prescribed interface, comply with prescribed interface standards or participate in prescribed interface arrangements when providing or receiving data which is required to be provided by data regulations. Such rules could include requiring data holders to comply with a certain API standard, for example. Subsection (1)(b) provides that rules may require persons described in the regulations to use a prescribed interface, comply with prescribed interface standards or participate in prescribed interface arrangements when, in the course of business, they receive data from a financial services provider that is required to be provided by data regulations. Subsection (1)(c) provides that rules may impose interface-related requirements on persons falling within subsection (3).

265 Subsection (3) defines the categories of person to which the interface-related requirements can apply. This includes interface bodies, persons required to set up interface bodies and persons who use related interfaces, standards or arrangements or are required to do so. The application is limited to interface bodies, and interfaces, standards and arrangements linked to the financial services sector (see subsection (5)).

266 Subsection (4) sets out the types of interface-related requirements that the FCA may impose. These include requirements relating to the composition, governance or activities of an interface body linked to the financial services sector. Subsection (5) details when an interface body, an interface, interface standards and interface arrangements are considered to be linked to the financial services sector.

267 Subsection (6) permits the Treasury via regulations to enable or require the FCA to impose additional requirements on firms to whom its rules apply. The intention of this is to allow the FCA to effectively regulate firms and interface bodies and intervene where necessary.

268 Subsection (7) provides that the FCA may impose requirements by notice or direction.

269 Subsection (8) and subsection (9) confirm that the same restrictions on powers of investigation apply to the FCA interface rules and requirements as apply under clause 9.

270 Subsection (10) provides definitions of "financial services provider" and "prescribed" in respect of the clause.

Clause 15: The FCA and financial services interfaces: supplementary

271 Clause 15 sets out provisions that regulations made by the Treasury under clause 14 may or must contain. The intention of these provisions is to set appropriate parameters for the sub-delegation of rulemaking powers from the Treasury to the FCA via regulations.

272 Subsection (2) permits regulations to require or enable the FCA to impose any interface requirement that could be imposed by regulations made under clause 7(4) or (5), but with the exception that the FCA may not enable or require a person to set up an interface body (only the Treasury may do that via regulations).

273 Subsection (3) requires that regulations must specify the purposes which the FCA must advance when exercising functions, matters to which the FCA must have regard, and provisions about the procedure for the making of any FCA interface rules.

274 Subsection (4) provides that regulations may impose requirements and make provision in relation to the FCA's exercise of any sub-delegated rulemaking powers. This might include, for example, requiring the FCA to carry out a costs benefit analysis in relation to the rules, requiring it to modify or waive the rules as they apply in a particular case, or requiring it to publish guidance about how it proposes to exercise its functions.

275 Subsection (5) provides that regulations may require or enable the FCA to impose requirements on a person to review conduct, take remedial action and to make redress for loss or damage suffered as a result of misconduct. Subsection (12) clarifies the things that redress may include.

276 Subsection (6) allows regulations to require or enable the FCA to make rules about the fees that persons listed in subsection (7) must pay to an interface body or another person listed in that subsection, to meet expenses described in subsection (8). This is to ensure that the FCA can require interface bodies and arrangements to be adequately and sustainably funded.

277 Subsection (7) provides that fees may be required to be paid by persons within clause 14(3)(b) or (c) or financial services providers.

278 The expenses described in subsection (8), for which rules may enable fees to be charged under subsection (6), are expenses incurred, or to be incurred, by the interface body or persons listed in subsection (7), or by persons acting on their behalf, in the conduct of functions imposed or conferred on them by Part 1 regulations or FCA interface rules.

279 Subsection (9) includes provisions that regulations must or may provide in relation to rules providing for such fees.

280 Subsection (10) provides that regulations may provide that the FCA's powers to make interface rules includes powers to do things described in section 21(1)(a) to (h), for example to make different provision in relation to different purposes or areas, or for particular cases, and that the restriction in relation to fees in clause 21(3) does not apply.

281 Subsection (11) provides relevant definitions.

Clause 16: The FCA and financial services interfaces: penalties and levies

282 Clause 16 makes provision about regulations that the Treasury may make providing for the FCA to impose financial penalties.

283 Subsection (2) makes provision about the way in which the FCA may be required or enabled to set penalties by regulations. The FCA may set the amount or maximum amount of a penalty

or set the method for calculating such amount. Subsection (3) sets out provisions that such regulations may or must make in relation to the FCA's policy in setting financial penalties.

284 Subsection (4) permits the Treasury to impose, or provide for the FCA to impose, a levy on data holders or third-party recipients for the purpose of meeting expenses incurred by the FCA, or a person acting on its behalf, in performing functions imposed or conferred by regulations under clause 14. This is to allow the FCA to recover expenses arising from its regulatory functions under Part 1. The regulations may make provision about what may or must be done with the funds. Subsection (5) provides that only directly affected persons should be subject to the levy. Subsections (6) and (7) confirm that the same requirements apply to regulations providing for this FCA levy, as apply to regulations for other levies in Part 1.

Clause 17: The FCA and co-ordination with other regulators

285 Clause 17 enables the Treasury to make regulations amending section 98 of the Financial Services (Banking Reform) Act 2013. Regulations may amend the definition of "relevant functions" to add or remove a function conferred on the FCA by regulations under Part 1 or amend the definition of "objectives" to add or remove an objective of the FCA relevant to such a function. This is intended to ensure that the FCA's functions under Part 1 regulations can be brought within scope of existing arrangements for co-ordination between the regulators of payment systems under Part 5 of the 2013 Act.

Supplementary

Clause 18: Liability in damages

286 Clause 18 permits the Secretary of State or the Treasury to make regulations to provide that a public authority cannot be liable in damages when they exercise their functions under Part 1. This power is conferred to ensure that a public authority can carry out its functions effectively and derives from the exemption from liability in damages for the FCA under the Financial Services and Markets Act 2000 which prevents the FCA from the need to defend vexatious claims that are a significant resource burden.

287 Subsection (2) lists the types of person eligible to be excluded from liability.

288 Subsection (3) ensures that liability cannot be excluded where person has acted in bad faith or if this would conflict with the Human Rights Act 1998, reflecting the FSMA 2000 provision.

Clause 19: Duty to review regulations

289 Subsections (1) and (2) of clause 19 require (subject to the exceptions in subsection (8)) the Secretary of State and the Treasury ("the relevant person"), by regulations, to provide for review of provisions made by them in other Part 1 regulations ("Part 1 provision").

290 Under subsection (3), the regulations must require review of the Part 1 provision in question, followed by publication of a report setting out the findings of that review and the laying of a copy of the report before Parliament. The intention is to give Parliament ongoing oversight of smart data schemes after they are introduced.

291 Under subsection (4), the regulations must require the first report to be published within five years of the of the Part 1 provision coming into force and the publication of subsequent reports at intervals of no more than five years, the intention being that smart data schemes are reviewed at least once every five years.

292 Subsection (5) deals with the criteria against which the regulations must require the review to be conducted. In all cases, the regulations must require the relevant person to consider whether the Part 1 provision in question remains appropriate. That must be assessed having regard to whether the provision continues to achieve the objectives it is intended to be achieved but may also be assessed having regard to other matters. Where that provision is part of data regulations, the review must have regard to the matters to which the regulation-maker was required to have regard in clauses 2(5) and 4(5).

293 Subsection (6) requires the regulations to provide that the published report omits material that the relevant person thinks might harm a person's commercial interests.

294 Subsection (7) allows the regulations to provide for a joint review and report in respect of Part 1 provisions made respectively by the Secretary of State and the Treasury.

295 Subsection (8)(a) and (b) is intended to disapply the review requirement in relation to regulations which amend Part 1 regulations ("substantive regulations") to which the review provision already applies, the intention being that provisions inserted (or otherwise modified) in the substantive regulations will be reviewed in accordance with the existing review requirements and timetable of the substantive regulations. Subsection (8)(c) ensures that the relevant person is not required to review revoked provisions.

296 Subsection (9) disapplies the review requirements in section 28 of the Small Business, Enterprise and Employment Act 2015 to avoid multiple review requirements.

Clause 20: Restrictions on processing and data protection

297 Subsection (1) of clause 20 ensures that, except as provided for by subsection (2) in relation to data protection, Part 1 regulations may provide for the processing of information not to be in breach an obligation of confidence (paragraph (a)) or any other restriction on the processing of information (paragraph (b)).

298 Subsection (2) provides that Part 1 regulations are not to be read as authorising or requiring processing of personal data that would contravene the data protection legislation. However, in determining whether processing of data would do so, account may be taken of the requirements of those regulations. Subsection (3) defines "the data protection legislation" and "personal data" by reference to the DPA 2018.

299 Subsections (1) and (2) reflect the provisions relating to pensions dashboards inserted by the Pension Schemes Act 2021 at section 238B(6) and (7) of the Pensions Act 2004.

Clause 21: Regulations under this Part: supplementary

300 Subsection (1) is largely self-explanatory. However, readers may, in particular, wish to note the following provisions.

301 Paragraph (f) allows Part 1 regulations to make provision by reference to standards, arrangements, specifications or technical requirements as published from time to time. This reflects section 238A(5)(a) of the Pensions Act 2004 relating to pensions dashboards. The purpose of this provision is, in particular, to allow for technical requirements by reference to published standards that are updated in line with developments in information technology.

302 Paragraph (g) allows the regulations to confer functions on a person which may include the exercise of a discretion and to make related procedural provisions. The ability to confer discretions reflects section 91(1)(b) of the Enterprise and Regulatory Reform Act 2013, which Part 1 of this Bill replaces, and section 238A(6) of the Pensions Act 2004.

303 Subsection (2) prevents Part 1 regulations from requiring or enabling a person to set the maximum amount of a fine, but regulations may refer to the standard scale, the statutory maximum or a similar amount.

304 Subsection (3) prevents Part 1 regulations (except where otherwise provided for by clauses 15 and 16 in relation to the FCA) from requiring or enabling a person to set the amount or maximum amount of a penalty or fee or the method by which that amount may be determined or, likewise, to set the amount, maximum amount or method of any increase of a penalty or fee. However, subsection (4)(a) enables the regulations to provide for that amount or method by reference to a published index. Subsection (4)(b) enables the regulations to require or enable a person to make decisions, within the framework of the maximum or methodology, about the amount payable, or increase, in a particular case.

305 Subsection (5) allows for amendment, repeal or revocation of primary legislation (as defined in clause 25(1)) in limited circumstances, these being to make provision about handling of complaints, dispute resolution and appeals and for provisions under subsection (1)(h) (incidental, supplementary, consequential, transitional or saving provisions). It is envisaged that subsection (5) might, for instance, be used to extend any statutory dispute resolution scheme in a specific sector to any smart data scheme which applies to that sector.

Clause 22: Regulations under this Part: Parliamentary procedure and consultation

306 Subsection (1) specifies the circumstances in which Part 1 regulations must be subject to affirmative Parliamentary scrutiny.

307 Under paragraphs (a) and (b), affirmative scrutiny is required for the first regulations under clauses 2(1), (3) and (4) and 4(1), (3) and (4) making provision about a particular description of customer data or business data. It is intended that regulations introducing a smart data scheme will be subject to affirmative scrutiny.

308 Under paragraph (c), affirmative scrutiny is required for regulations which make requirements more onerous for data holders or interface bodies.

309 Under paragraph (d), affirmative scrutiny is required where regulations are made under, or in reliance on, the following clauses:

- clause 6(5) (monitoring power of a decision-maker);
- clause 7 (interface bodies);
- clause 8 (enforcement);
- clause 11 (fees);
- clause 12 (levy);
- clause 14 (the FCA and financial services interfaces);
- clause 16 (the FCA and financial services interfaces: penalties and levies);
- clause 17 (the FCA and co-ordination with other regulators);
- clause 18 (liability in damages).

310 Under paragraph (e), affirmative scrutiny is required for regulations to which clause 21(5) applies, which amend, repeal or revoke primary legislation.

311 Subsection (3) 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, or their representatives;
- sectoral regulators with functions in relation to data holders under the proposed regulations.

312 Subsection (4) clarifies that, in making regulations, the Secretary of State or the Treasury can rely on a consultation which takes place before this clause comes into force.

313 Neither the consultation obligation in subsection (3) nor anything else in Part 1 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 23: Related subordinate legislation

314 Clause 23 provides that the regulation-making powers in Part 1 may be exercised so as to make, in connection with other data provision in subordinate legislation, any provision that they could be exercised to make as part of, or in connection with, provision made under clauses 2(1) to (4) or 4(1) to (4). This is intended to allow smart data provision to be made by amending, or making provision consequential to, existing subordinate legislation, rather than making stand-alone regulations. This could include for example amending existing data sharing requirements in financial services legislation such as open banking provisions in the Payment Services Regulations 2017.

Clause 24: Repeal of provisions relating to supply of customer data

315 Clause 24 repeals sections 89 to 91 (supply of customer data) of the Enterprise and Regulatory Reform Act 2013, which Part 1 replaces.

Clause 25: Other defined terms

316 Subsection (1) of clause 25 defines terms which have not been defined elsewhere in Part 1. Some of these definitions are referred to in these notes in the context of specific clauses. Readers should, in particular, note the definition of "specified" in relation to the contexts in which that clause is used and "third party recipient" which may refer to a third party recipient for customer data (clause 4(2)), business data (clause 4(2)) or both according to the context.

317 Subsection (2) explains what is meant by references in Part 1 to something being done "in the course of business".

Clause 26: Index of defined terms for this Part

318 Clause 26 sets out an index of terms defined in Part 1.

Part 2: Digital Verification Services

Introductory

Clause 27: Introductory

319 Clause 27 sets out the scope of Part 2 of the Bill and defines digital verification services (DVS).

DVS trust framework and supplementary codes

Clause 28: DVS trust framework

320 Subsection (1) requires the Secretary of State to prepare and publish a DVS trust framework document (the 'trust framework') which sets out rules concerning the provision of DVS.

321 Subsection (2) makes clear that those rules may include the conduct of a person providing such services and that references in this Part to a person providing services in accordance with the trust framework (or similarly expressed) include compliance with the rules contained in that framework relating to that person and/or their conduct.

322 Subsection (3) requires the Secretary of State to consult the Information Commissioner and any persons the Secretary of State considers appropriate when preparing the trust framework, while subsection (4) makes clear that this consultation can take place before this section comes into force.

323 Subsection (5) enables the Secretary of State to revise and republish the trust framework following a review under clause 31, or at other suitable times.

324 Subsection (6) sets out that the trust framework, or a revised version of the trust framework, must state when it will come into force, and this cannot be before the relevant trust framework is published. Subsection (7) states that the trust framework or a revised version of the trust framework can set different rules for different digital verification services, , can specify that provisions come into force at different times for different purposes, and can include transitional or saving provisions.

325 Subsections (8) to (10) set out that when the trust framework is revised, provisions in the revised and republished trust framework can specify that from a particular date or from the end of a period, certificates that were issued to organisations confirming they provide services in accordance with the trust framework before the changes come into force (pre-revision certificates) do not count for specified purposes. Such provisions may specify different terms for different pre-revision certificates.

Clause 29: Supplementary codes

326 Subsection (1) enables the Secretary of State to prepare and publish additional sets of rules applicable to specific DVS use cases that supplement the trust framework. Subsection (2) notes that such published sets of rules will be called 'supplementary codes'.

327 Subsection (3) sets out that supplementary codes may include rules relating to the provision of services and to the conduct of a person providing such services. This subsection also clarifies that references in this Part to a person providing services in accordance with a supplementary code (or similarly expressed) include compliance with the rules contained in the supplementary code relating to that person and/or their conduct.

328 Subsection (4) requires the Secretary of State to consult the Information Commissioner and any persons the Secretary of State considers appropriate to consult when preparing supplementary codes. Subsection (5) sets out that this consultation can take place before this section comes into force.

329 Subsection (6) enables the Secretary of State to revise and republish supplementary codes following a review under clause 31, or at other suitable times.

330 Subsection (7) sets out that a supplementary code or a revised version of a supplementary code must state when it will come into force, and this cannot be before the relevant supplementary code is published. Subsection (8) states that a supplementary code or a revised version of a supplementary code can set different rules for different digital verification services, can specify that provisions come into force at different times for different purposes, and can include transitional or saving provisions.

331 Subsections (9) to (11) set out that when a supplementary code is revised, provisions in the revised and republished supplementary code can specify that from a particular date or from the end of a period, certificates that were issued to organisations confirming they provide services in accordance with the relevant supplementary code before the changes come into force (pre-revision certificates) do not count for specified purposes. Such provisions may specify different terms for different pre-revision certificates.

Clause 30: Withdrawal of a supplementary code

332 Clause 30 allows the Secretary of State to make a determination to withdraw a supplementary code. Such determination must be published, and must specify when the supplementary code will be withdrawn. The specification of when the supplementary code is withdrawn must be a time after the end of 21 days following publication of the determination (starting on the day of publication).

Clause 31: Review of DVS trust framework and supplementary codes

333 Clause 31 sets out that the trust framework and each supplementary code should be reviewed at least every 12 months, in consultation with the Information Commissioner and any persons the Secretary of State considers appropriate to consult. Subsection (1)(b) makes it clear that this obligation does not apply to withdrawn supplementary codes.

DVS register

Clause 32: DVS register

334 Subsections (1), (2) and (3) of clause 32 require the Secretary of State to establish and maintain a publicly available DVS register ('the register') of persons providing digital verification services.

Clause 33: Registration in the DVS register

335 Subsection (1) provides that a person must be registered if they hold a certificate issued by an accredited conformity assessment body confirming they are providing DVS in accordance with the trust framework, if they have applied to be registered in respect of one or more DVS for which they have a certificate, if they have complied with the registration requirements set out in a determination made under clause 38 and if they have paid any fee payable under clause 39(1).

336 Subsection (2) clarifies that registration in the register under subsection (1) is subject to the Secretary of State's power to refuse registration set out in clause 34(1) and his duties to refuse registration in clauses 34(10) and 41(11). Subsection (3) makes it clear that that the Secretary of State may not register a person if the requirements in subsection (1) are not met.

337 Subsection (4) also requires the Secretary of State to record on the register the services that a person is registered to provide.

338 Subsection (5) ensures that where a certificate has expired, has been withdrawn or is a pre-revision certificate required to be ignored under clause 28(8), the organisation cannot be registered.

339 Subsections (6) and (7) are self-explanatory and reference the regulations that govern the accreditation and conformity assessment bodies.

Clause 34: Power to refuse registration in the DVS register

340 Subsection (1) allows the Secretary of State to refuse to register a person in the DVS register if he considers it necessary in the interests of national security or is satisfied that the organisation is not compliant with the trust framework in respect of the digital verification services that the person has applied to be registered.

341 Subsections (2) and (3) set out that the Secretary of State must inform the person being refused registration via written notice of his intention to refuse the application. That notice must state the name and address of the recipient, the reasons for removal, the right to make written representations about the intention to refuse them registration, the date by which representations should be made and, if the intention is to prevent the organisation from re-applying within a certain period the notice must specify the period proposed, noting that a person may make representations about that period.

342 Subsection (4) sets out that where the Secretary of State is intending to refuse an application on national security grounds under subsection (1)(a), the requirement to provide a person with reasons under subsection (3) does not apply if giving such reasons would be contrary to the interests of national security.

343 Subsection (5) specifies that the person must be given a minimum of 21 days beginning on the day the notice is given within which to make written representations to the Secretary of State.

344 Subsection (6) provides that the person can make oral representation if the Secretary of State considers this appropriate. The ability to make oral representations should be stated in the written notice and the notice must give the person details of how and when the oral representation can be made. Subsection (7) requires that any written or oral representations made in accordance with the written notice must be considered by the Secretary of State when making a decision on refusal of registration.

345 Subsection (8) requires the Secretary of State to give written notice to a person informing them that their application for registration has been refused.

346 Subsection (9) allows the Secretary of State to include in the notice for refusal of registration under subsection (8) a period within which any subsequent application to be registered by that person will be refused and subsection (10) requires the Secretary of State to refuse an application for registration during that period. Subsection (11) sets out that the period of removal must start on the day the notice is given and not exceed two years.

Clause 35: Registration of additional services

347 Clause 35 allows registered DVS providers to apply to have their entries in the register amended to record they are providing additional services in accordance with the rules of the trust framework.

348 Subsection (1) sets out that a person may apply to register additional services in their existing entry on the register. Such an application may be made in respect of services for which the person holds a certificate issued by an accredited conformity assessment body confirming that they are providing those services in compliance with the rules of the trust framework. The application must comply with any requirements of a determination under clause 38 and a fee must be paid where required by regulations made under clause 39(1).

349 Subsection (2) requires the Secretary of State to amend the DVS register to record the additional services if the requirements in subsection (1) are met. Subsection (3) clarifies that that the Secretary of State may not register additional services if the conditions in subsection (1) are not met.

350 Subsection (4) ensures that where a certificate has expired, has been withdrawn or is a pre-revision certificate required to be ignored under clause 28(8), the additional services cannot be registered.

Clause 36: Supplementary notes

351 Clause 36 allows a person registered in the DVS register to apply to add a supplementary note to the register, which sets out that they are providing one or more services in accordance with the rules of a supplementary code.

352 Subsection (1) sets out what needs to be done when a person wants to have a supplementary note included in the DVS register. An application to have a supplementary note included in the DVS register must comply with any requirements of a determination under clause 38 and a fee must be paid where required by regulations under clause 39(1).

353 Subsections (2) and (3) require the Secretary of State to add a supplementary note in the DVS register where the requirements in subsection (1) are met, unless the supplementary code against which the application has been made has been withdrawn,

354 Subsection (4) clarifies that supplementary notes can only be added where the conditions in subsection (1) are met.

355 Subsections (5) provides that a certificate will not count if it has expired, been withdrawn, or the supplementary code to which it relates has been revised since the certificate was issued and the rules of the revised code specify that the certificate should not count. In those circumstances, the supplementary note cannot appear in the register.

356 Subsection (6) is self-explanatory.

Clause 37: Addition of services to supplementary notes

357 Clause 37 allows a person registered in the DVS register with supplementary notes in their register entries to apply to have their notes amended to include additional services.

358 Subsection (1) sets out what needs to be done when an organisation wants to have their supplementary note in the DVS register amended to record their provision of additional services. An application may be made for services for which the person holds a certificate issued by an accredited conformity assessment body confirming that they are providing those

services in compliance with a supplementary code. The application must comply with any requirements of a determination under Clause 38 and a fee must be paid where required by regulations made under clause 39(1).

359 Subsections (2) and (3) require the Secretary of State to amend the supplementary note in the register if the requirements in subsection (1) are met, unless the supplementary code against which the application has been made has been withdrawn.

360 Subsection (4) clarifies that that the Secretary of State may not amend a supplementary note if the conditions in subsection (1) are not met.

361 Subsection (5) provides that a certificate will not count if it has expired, been withdrawn, or is a pre-revision certificate required to be ignored under clause 29(9).

Clause 38: Applications for registration, supplementary notes, etc

362 Subsection (1) of clause 38 enables the Secretary of State to determine the form and manner in which applications to be registered on the DVS register, to add additional services to the DVS register, to include a supplementary note in the DVS register or to add services to a supplementary note may be made, including the information and documents to be provided in support of an application.

363 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 clause.

Clause 39: Fees for applications for registration, supplementary notes, etc

364 Subsection (1) enables the Secretary of State to make provision in regulations regarding the payment of fees in respect of applications made under clauses 33, 35, 36 or 37 for registration in the DVS register, addition of services or supplementary notes or services to supplementary notes in their entry on the DVS register, and for continued registration on the DVS register.

365 Subsection (2) clarifies that the regulations may not provide for the payment of fees to any party other than the Secretary of State.

366 Subsection (3) sets out that regulations must specify the amount of the fee to be paid, or the maximum amount at which a fee could be set, or provide for the fee or its maximum amount to be determined as set out in regulations.

367 Subsection (4) provides that the fees can be set at a level higher than the administrative costs of determining an application or the administrative costs associated with continued registration. This is so that fees may cover operating costs of the DVS framework.

368 Subsection (5) is a non-exhaustive list of the types of provisions the regulations made under subsection (1) may include, such as the timing of fees, the manner in which fees must be paid, the existence of discounts and exceptions to the requirement to pay a fee, if applicable, conditions on the refund of fees, and interest payable on unpaid fees. It also confirms that regulations made under subsection (1) may include provisions on conferring functions to the Secretary of State on all the mentioned items with the exception of interest payable on unpaid fees.

369 Subsection (6) sets out that fees payable for continued registration and interest on unpaid fees is recoverable summarily, or recoverable as a civil debt in Scotland.

370 Subsection (7) sets out that the regulations made under subsection (1) can make different provisions for different purposes, and may make transitional, transitory or saving provision.

371 Subsection (8) clarifies that regulations made under this section will be subject to the negative resolution procedure.

Clause 40: Duty to remove person from the DVS register

372 Subsection (1) requires the Secretary of State to remove a person from the register when the person asks to be removed or stops providing all of the DVS for which they are registered, or no longer holds a certificate from an accredited conformity assessment body that certifies at least one of the DVS they provide as compliant with the trust framework.

373 Subsection (2) provides that a certificate will not count for that purpose if it has expired, has been withdrawn or is a pre-revision certificate required to be ignored under clause 28(8).

Clause 41: Power to remove person from the DVS register

374 Subsection (1) enables the Secretary of State to remove a person from the register in certain circumstances. First, if the Secretary of State is satisfied that the person is failing to comply with the trust framework when providing one or more of the DVS for which they are registered. Second, if the person has a supplementary note in the register, and the Secretary of State is satisfied that they are failing to comply with the relevant supplementary code in their provision of one or more of the DVS for which they are registered. Third, if the Secretary of State is satisfied that the person has failed to provide information to the Secretary of State where a notice has been issued under clause 51. Fourth, if the Secretary of State considers it necessary in the interests of national security.

375 Subsections (2) and (3) require the Secretary of State to give written notice to the person of an intention to remove them from the register. That 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, if the intention is to prevent the person from re-applying within a certain period, the notice must specify the period proposed, noting that a person may make representations about that period.

376 Subsection (4) sets out that where the Secretary of State is intending to refuse an application on national security grounds under subsection (1)(d), the requirement to provide a person with reasons under subsection (3) does not apply if giving such reasons would be contrary to the interests of national security.

377 Subsection (5) specifies that the person has a minimum of 21 days beginning on the day the notice is given within which to make written representations to the Secretary of State.

378 Subsection (6) provides that the person can make oral representation if the Secretary of State considers this appropriate. The ability to make oral representations should be stated in the written notice and the notice must give the person details of how and when the oral representation can be made.

379 Subsection (7) requires that any written or oral representations made in accordance with the written notice must be considered by the Secretary of State when deciding whether to remove a person from the DVS register.

380 Subsection (8) requires the Secretary of State to give written notice to a person informing them they have been removed from the register.

381 Subsection (9) allows the Secretary of State to include in the notice for refusal of registration under subsection (8) a period within which any subsequent application made by the person to be re-registered will be refused and subsection (10) requires the Secretary of State to refuse an application for re-registration during that period. Subsection (11) sets out that the period of removal must start on the day the notice is given and not exceed two years.

Clause 42: Duty to remove services from the DVS register

382 Subsections (1) and (2) set out that if a person asks for an amendment to reflect that they no longer provide one or more registered services, if they stop providing one or more of the registered services (but not all of them), or if they are no longer certified by an accredited conformity assessment body for all of the services for which they are registered, the Secretary of State must amend the register accordingly to remove the relevant services.

383 Subsection (3) sets out that a certificate will not count if it has expired, has been withdrawn, or is a pre-revision certificate required to be ignored under clause 28(8).

Clause 43: Duty to remove supplementary notes from the DVS register

384 Subsection (1) sets out that if a person with a supplementary note in the register asks for the note to be removed, if they stop providing all of the services to which the note relates, if they are no longer certified to be compliant with a supplementary code by an accredited conformity assessment body for at least one of the services in the note, or if they continue to be certified to be compliant but the relevant supplementary has been withdrawn, the Secretary of State must amend the register to remove the relevant supplementary note.

385 Subsection (2) sets out that a certificate will not count if it has expired, has been withdrawn, or is a pre-revision certificate required to be ignored under 29(9).

Clause 44: Duty to remove services from supplementary notes

386 Subsections (1) and (2) set out that if a person with a supplementary note on the DVS register asks for services listed on the note to be removed, if they stop providing one or more of the services listed on the note, if they are no longer certified as compliant with a supplementary code by an accredited conformity assessment body for all of the services in the note, the Secretary of State must amend the register to remove the relevant service or services from the supplementary note.

387 Subsections (3) and (4) set out that a certificate will not count if it has expired or has been withdrawn or is a pre-revision certificate required to be ignored under 29(9).

Information Gateway

Clause 45: Power of public authority to disclose information to registered person

388 Subsections (1) and (2) state that a public authority may share information relating to an individual with a person registered in the DVS register, where the individual makes a request to that person to provide DVS.

389 Subsection (3) sets out that information disclosed under this clause does not breach any duty of confidentiality owed by the public authority making the disclosure or any other restrictions (however imposed) relating to the disclosure of information.

390 Subsection (4) does not authorise disclosure by a public authority that would breach data protection legislation, although the power to disclose information under this clause is to be taken into account in deciding whether the disclosure would breach data protection

legislation. Similarly, it does not authorise disclosure of information which is prohibited under Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.

391 Subsection (5) makes clear that public authorities may only disclose information which they have obtained through exercising functions of a public nature.

392 Subsection (6) provides that this clause does not affect any powers to disclose information that exist apart from this section.

393 Subsection (7) enables public authorities to charge fees for disclosing information to persons providing DVS.

394 Subsection (8) defines the terms "data protection legislation" and "public authority" for the purpose of this section.

Clause 46: Information disclosed by the Revenue and Customs

395 Subsections (1) and (2) set out that where HMRC have disclosed personal information to a person to enable provision of DVS for an individual under clause 45, the person must not further disclose that information otherwise than for the purpose of providing DVS for the individual, without the consent of the Commissioners for HMRC.

396 Subsection (3) sets out that if a third party receives the information disclosed by HMRC to the registered person providing DVS directly or indirectly from the person to whom the information was disclosed by HMRC, the third party must not further disclose the information without consent of the Commissioners for HMRC.

397 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 clause.

398 Subsection (5) defines the terms "personal information" and "the Revenue and Customs" for the purpose of this section.

Clause 47: Information disclosed by the Welsh Revenue Authority

399 Clauses (1) and (2) provide that where the Welsh Revenue Authority discloses personal information to a person under clause 45 to enable provision of DVS for an individual, the person must not further disclose the information otherwise than for the purpose of providing DVS, without the consent of the Welsh Revenue Authority.

400 Subsection (3) sets out that if a third party receives the information disclosed by the Welsh Revenue Authority to the registered person providing DVS directly or indirectly from the person to whom the information was disclosed by the Welsh Revenue Authority, the third party must not further disclose the information without consent of the Welsh Revenue Authority.

401 Subsection (4) sets out that it is an offence to disclose information in contravention of subsections (2) and (3). 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.

402 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.

403 Subsection (7) defines the term "personal information" for the purpose of this section.

Clause 48: Information disclosed by Revenue Scotland

404 Clauses (1) and (2) set out that where Revenue Scotland discloses personal information to a person under clause 45 for the purpose to enable provision of DVS to an individual, that person must not further disclose that information otherwise than for the purpose of providing DVS, without the consent of Revenue Scotland.

405 Subsection (3) sets out that if a third party receives the information disclosed by Revenue Scotland to the registered person providing DVS directly or indirectly from the person to whom the information was disclosed by Revenue Scotland, the third party must not further disclose the information without consent of Revenue Scotland.

406 Subsection (4) sets out that it is an offence to disclose information in contravention of subsections (2) and (3).

407 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.

408 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.

409 Subsection (7) defines the term "personal information" for the purposes of this section.

Clause 49: Code of practice about the disclosure of information

410 Subsection (1) sets out that the Secretary of State must prepare and publish a code of practice regarding the disclosure of information under clause 45. 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 45.

411 Subsection (4) enables the Secretary of State to revise and republish the code of practice.

412 Subsection (5) requires the Secretary of State to consult the Information Commissioner, the devolved administrations, and any persons the Secretary of State considers appropriate before preparing or revising the code of practice.

413 Subsection (6) states that the consultation exercise may be carried out before this section comes into force.

414 Subsections (7) and (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.

415 Subsections (9), (10) and (11) provide definitions relevant to the clause.

Trust mark

Clause 50: Trust mark for use by registered persons

416 Section (1) provides that the Secretary of State can designate a trust mark to be used in providing or offering to provide DVS. Section (2) states that the Secretary of State must publish the trust mark. Section (3) provides that 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 and section (4) states that the Secretary of State can enforce subsection (3) in civil proceedings.

Supplementary

Clause 51: Power of Secretary of State to require information

417 Clause 51 provides that the Secretary of State may by written notice require an accredited conformity assessment body or a person included in 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.

418 Subsection (2) sets out that the written notice must explain why the information is required and subsection (3) makes further provision about what may be contained in the written notice.

419 Subsection (4) makes clear that the written notice must provide information about the consequences of failing to comply with the notice.

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

421 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.

422 Subsection (7) sets out that the disclosure of information requested by the Secretary of State must not infringe restrictions under clauses 46, 47 or 48 of this Part, data protection legislation or specified sections of the Investigatory Powers Act 2016.

423 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. Subsection (12) defines the term "data protection legislation" for the purpose of this section.

Clause 52: Arrangements for third party to exercise functions

424 Clause 52 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. Should such arrangements be made, references to the Secretary of State in this Part, or regulations made under this Part, must be read accordingly.

425 Subsection (2) makes clear that arrangements made under this clause may provide for the Secretary of State to make payments to the person and make provision for the circumstances in which those payments are to be repaid to the Secretary of State. Subsection (3) states that

regulations made under this clause are subject to the affirmative procedure. Subsection (4) defines the term "relevant function" for the purposes of this section as all functions conferred by or under this Part, with the exception of the power to make regulations.

426 Subsection (5) clarifies that if arrangements are made under this section to delegate the function of charging or recovering fees to a prescribed person, such person must pay the fees to the Secretary of State unless the Secretary of State has directed otherwise.

Clause 53: Report on the operation of this Part

427 Clause 53 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 clause 28 coming into force and thereafter reports must not be published more than 12 months apart.

Clause 54: Index of defined terms for this Part 2

428 Clause 54 is an index of terms which are defined in Part 2.

Clause 55: Powers relating to verification of identity or status

429 Subsections (1), (2) and (3) of section 55 each elaborate and expand on the parameters of existing order/regulation-making powers to prescribe requirements, right to work checks and documents in section 15(3) of the Immigration, Asylum and Nationality Act 2006, section 34 of the Immigration Act 2014 and paragraph 5(6)(b) and (c) of Schedule 6 to the Immigration Act 2016. The examples of the way these powers may be exercised include by making provision that specifies/prescribes documents provided to, and generated by, a person in the DVS register established under Part 2 of the Bill (a DVS-registered person) and to specify/prescribe steps and checks involving the use of services by such a person. New provisions are also inserted into these order/regulation-making powers that confer powers to specify/prescribe a description of DVS-registered person whose entry in the DVS register includes a supplementary note relating to specified/prescribed services.

Part 3: National Underground Asset Register

Clause 56: National Underground Asset Register: England and Wales

430 Subsection (1) of this clause inserts a new Part 3A into the New Roads and Street Works Act 1991 ("the 1991 Act") which, among other things, requires the Secretary of State to keep a register of information relating to apparatus in streets in England and Wales (to be known as the National Underground Asset Register ("NUAR")). The sections comprising the new Part 3A set out a legislative framework for NUAR, including empowering the Secretary of State to make provision by regulations in connection with granting access to information kept in NUAR, the payment of fees by undertakers in relation to NUAR, requiring undertakers to provide information to the Secretary of State for the purposes of regulations, monetary penalties and arrangements for third parties to exercise relevant functions of the Secretary of State.

431 The new Part 3A inserted into the 1991 Act comprises new sections 106A to 106J; each of these is considered in turn below.

Section 106A: National Underground Asset Register

432 A key aspect of the new legislative framework for NUAR is the requirement, imposed by section 106A(1) to be inserted into the 1991 Act, for the Secretary of State to keep a register of information relating to apparatus in streets in England and Wales. This register is referred to

in the Act as "NUAR" (as defined by subsection (2)) and will be the central repository of information into which, in accordance with other provisions being inserted into the 1991 Act, certain persons will be required to enter information. In practice, NUAR will be a digital register and the information within it will be used to form a digital underground map displaying information about apparatus "in" a street.

433 Subsection (3) confers on a power on the Secretary of State to prescribe, through regulations, the form and manner in which NUAR must be kept. Regulations under this subsection are subject to the negative procedure as provided for in subsection (5).

434 Clause 57 makes a number of amendments to the 1991 Act, some of which will require people to enter information into NUAR. In order to facilitate this, and as required by subsection (4), the Secretary of State must ensure such people have access to NUAR.

435 Clause 58 (3) inserts Article 45A(1) into the Street Works (Northern Ireland) Order 1995. This imposes an obligation on the Secretary of State, equivalent to that set out in section 106A in relation to England and Wales, to keep a register of information relating to apparatus in streets in Northern Ireland. Subsection (6) allows the Secretary of State to discharge both obligations by keeping a single register which covers England, Wales and Northern Ireland.

Section 106B: Initial upload of information into NUAR

436 For NUAR to be a reliable and comprehensive source of information it is crucial that, from the outset, it also contains existing information which is already held in undertakers' records.

437 This section establishes the concept of the "initial upload period", during which undertakers having apparatus in a street must enter into NUAR all information that is already included in their records on a specific date, referred to in this provision as the "archive upload date". Such undertakers must also, during this period, enter into NUAR any other information, held by the undertaker on that date, of a description prescribed by the Secretary of State in regulations.

438 The Secretary of State may also, in regulations made under subsections (2) and (3) respectively, set out when this duty to enter information held in their records into NUAR does not apply, and the form and manner in which this information must be entered into NUAR for these purposes.

439 Subsection (8)(a) imposes a duty on the Secretary of State to specify, in regulations, the "archive upload date" (on which a "snapshot" of relevant information in the undertaker's records is taken). Subsection (8)(b) also requires the Secretary of State to specify the duration of the "initial upload period", beginning with the archive upload date, within which the information comprising that snapshot must be entered into NUAR.

440 An undertaker who fails to comply with a duty imposed by section 106B commits a criminal offence which is triable summarily and, if convicted, can result in a fine.

Section 106C: Access to information kept in NUAR

441 This section sets out the approach through which information held within NUAR can be made available to others. The policy intent is to make NUAR data available to planners and excavators for the purposes of carrying out safe and efficient excavations. However, undertakers currently make their data available to other persons for other purposes. This provision ensures NUAR data can be used, if considered appropriate, for additional purposes.

442 Subsections (1) and (2) provide that the Secretary of State may, by regulations, determine who can access information kept in NUAR, including by specifying what information is shared, with whom, for what purpose and in what form and manner. This section also empowers the Secretary of State to make provision for such information to be made available for free or for a fee. So, for example, the Secretary of State could provide for information held in NUAR to be accessible by undertakers for the purpose of carrying out street works excavations.

443 Subsection 2(h) establishes that the Secretary of State would have the ability to make provision for the granting of licences by the Secretary of State in relation to any non-Crown IP rights (as defined by subsection (5)) that may exist in relation to information made available from NUAR. Licences in relation to Crown IP rights would be managed by the Keeper of the National Archives.

444 Subsection (3) makes provisions to clarify that, as a general approach, the processing of information in exercise of functions under sections 106A does not breach any obligation of confidence or any other restriction, however imposed. In most cases, this general approach will be essential for the effective and efficient running of NUAR. However, there could also be circumstances, which become apparent over time, in which it would not be appropriate for this general approach to apply. New section 106C(3) permits the Secretary of State, through regulations, to prescribe exceptions to this approach where considered appropriate to do so. Subsection (3) also makes clear that this general approach is nevertheless subject to the provision made by section 106H; as explained below, the general approach does not override or otherwise take priority over the requirements of the data protection legislation. "Processing" of information, for these purposes, has the same broad meaning as in the DPA 2018.

Section 106D: Fees payable by undertakers in relation to NUAR

445 Once the NUAR service as provided for by these new legislative provisions is operational, the policy intent is for its running costs to be funded through fees paid by those who benefit from the service, rather than being funded by the taxpayer.

446 Through regulations made under subsection (1), the Secretary of State may create a fees scheme for these purposes. This scheme may require undertakers with apparatus in a street to pay fees to fund the operation of the NUAR service. Such an approach reflects the benefit that such undertakers will receive through the removal of the requirement, currently set out at section 79(3) of the 1991 Act, to make their records of information relating to their apparatus available to others.

447 The Secretary of State will have a number of options available when setting the amount of fees to be payable under the scheme, as set out in subsection (2). The specific amount (or amounts) of fees may be set out in the regulations themselves. Or the Secretary of State can set out in regulations the maximum amounts of the fees, or a method through which specific or maximum amounts of fees can be determined. The Secretary of State is able to make different provision for different purposes (see section 106I(2)); in practice, this will enable, if considered appropriate, a "tiered" approach through which undertakers are allocated a tier and charged a particular fee based on this.

448 If the regulations adopt an approach other than specifying the actual amounts of fees, then the Secretary of State must set out the actual amounts in a statement which is to be published and laid before Parliament, as required by subsection (4). As a result, whatever approach is taken, the actual amounts of fees that apply in any particular case will be readily available to those required to pay them.

449 In general terms, subsection (3) imposes a requirement on the Secretary of State, when making regulations under subsection (1), to seek to ensure that – so far as possible and taking one year with another - the fees being imposed match the costs of running NUAR. This reflects the intended approach through which such fees will be targeted at covering such costs but not generate additional revenue beyond this. Subsection (10) clarifies that this balancing exercise includes fees imposed through regulations made under section 106D(1) of the 1991 Act and Article 45D(1) of the 1995 Order ("combined NUAR income"), and the expenses incurred in running the service across England, Wales and Northern Ireland ("combined NUAR expenses"). This reflects the intention for NUAR to operate as a single service across the three nations.

450 Before making regulations relating to a fee scheme, the Secretary of State must first comply with the consultation requirements set out at subsection (6). These require consultation with representatives of persons likely to be affected by the fee scheme, and such other persons as the Secretary of State considers appropriate.

Section 106E: Providing information for purposes of regulations under section 106D

451 In developing and then operating the fees scheme described above, it is likely that the Secretary of State will need to consider a range of different types of information. Section 106E enables the Secretary of State to impose legally binding requirements on undertakers to provide such information for two main purposes.

452 The Secretary of State may require information from undertakers in order to enable the fees scheme to be developed, or to inform decisions about changes that could be made to the scheme once it is up and running. For example, if a "tiered" approach of the type described above were to be adopted, specific information from undertakers could be required in order to determine how such tiers should be described. Subsection (1) enables the Secretary of State to make regulations for this purpose.

453 Subsection (2) provides a second power to require information from undertakers. This can be used to request information relevant to more "operational" aspects of the fees scheme, once it has been set up through regulations made under section 106D(1). More specifically, information can be requested in order to ascertain whether a fee is payable by a person under the fees scheme and, if so, enable the amount of such fee to be calculated.

454 In addition to requesting information, subsection (3) makes clear that such regulations can also require undertakers to update the Secretary of State about any changes to that information after it has been provided. Further, subsection (4) provides that such regulations may also set out when (and with what frequency) information is to be provided by undertakers, and the form and manner in which information is to be provided. The regulations can also set out exceptions to any requirements to provide information that the regulations imposed.

Section 106F: Monetary Penalties

455 This section gives effect to the new Schedule 5A, found at Schedule 1 to the Bill, which is to be inserted into the 1991 Act. Schedule 5A makes provision for the Secretary of State to impose monetary penalties as a means of enforcing any requirements to pay fees, or provide information, as set out in regulations made under new sections 106D(1), 106E(1) or 106E(2).

Section 106G: Arrangements for third party to exercise functions

456 The new Part 3A inserted into the 1991 Act confers a range of functions on the Secretary of State. A number of these functions concern operational aspects of running NUAR, such as the

keeping of the register, making information kept in the register available to others, and the receiving of fees. It is anticipated that, in practice, some of the Secretary of State's functions, save those set out in subsection (8)(a) and (b) of new section 106G inserted into the 1991 Act by this clause, can be appropriately exercised by others.

457 Section 106G(1) and (2) provides for this to be done through the Secretary of State entering into arrangements with one or more persons or organisations. This could mean arrangements providing for more than one person to exercise a function, or for different organisations to exercise different functions. In addition, as set out in subsection (5), the fact that the Secretary of State has entered into arrangements with others in relation to one or more functions does not prevent the Secretary of State from also exercising those functions. Specific provision is also made, in subsection (3), allowing such arrangements to provide for payments to be made by the Secretary of State to the other person or organisation (and to provide for circumstances in which any such payments must be repaid).

458 In light of the importance of the identity of such persons or organisations, the Secretary of State will only be able to enter into arrangements with a person where they have been identified, or "prescribed", in regulations for this purpose. Where arrangements have been entered into with a prescribed person or organisation, references to the Secretary of State in any of the provisions of the new Part 3A inserted into the 1991 Act, or in any regulations made under powers in that Part, are instead (or additionally) to be read as references to the person or organisation concerned insofar as required to reflect the detail of the arrangements.

459 Subsection (6) makes provision as to the disclosure of information between the Secretary of State and another party to arrangements under this section, setting out a general approach similar to that provided for in section 106C(3). Likewise, in this context, the Secretary of State is able to disapply this general approach, through the making of regulations, if considered appropriate, and this approach is also subject to section 106H.

460 Subsection (9) makes clear that if a party to arrangements under this section exercises the function of charging or recovering fees, the person must pay the fees to the Secretary of State, except to the extent that Secretary of State directs otherwise.

Section 106H: Data Protection

461 It is not anticipated that information processed for the purposes of NUAR will typically include personal data. However, should any processing of personal data take place as a result of the provision made by (or in regulations under) the new Part 3A being inserted into the 1991 Act, section 106H makes clear that this processing will have to be undertaken in accordance with the existing data protection legislation. In this context, both "personal data" and "the data protection legislation" have the same meaning as in the DPA 2018.

Section 106I: Regulations under this Part

462 New Part 3A confers a number of powers on the Secretary of State to make regulations, including where a provision refers to the Secretary of State "prescribing" certain things. Section 106I makes provision about how these regulation-making powers can be exercised in practice. This includes, at subsection (4) a requirement to consult the Welsh Ministers and the Department for Infrastructure in Northern Ireland before exercising these powers.

Section 106J: Interpretation

463 Section 106J defines various terms for the purposes of this Part.

464 Subsection (2) of clause 56 clarifies that section 166 of the 1991Act, so far as it relates to new Part 3A, extends to England and Wales.

465 Subsection (3) of clause 56 provides for the provisions of the new Part 3A inserted into the 1991 Act to bind the Crown and clarifies that this is not to be construed as authorising the bringing of proceedings for a criminal offence against a person acting on behalf of the Crown.

466 Subsection (4) of clause 56 gives effect to Schedule 1 which inserts new Schedule 5A into the 1991 Act. Schedule 5A sets out the legal framework through which the Secretary of State can impose monetary penalties in response to a failure to comply with any requirements set out in regulations made under sections 106D(1) and 106E(1) and 106E(2).

Clause 57: Information in relation to apparatus: England and Wales

467 Clause 57 amends section 79 of the 1991 Act, and replaces the existing (but not yet commenced) section 80 of that Act. The amendments to section 79, among other things, require undertakers to record certain information related to apparatus and to enter information into NUAR. The new Section 80 of the 1991 Act imposes duties on persons executing works of any description in a street to take other certain steps where they identify missing or incorrect information in existing records, or where they find apparatus and cannot ascertain its owner.

468 Section 79 of the 1991 Act already imposes a number of record-keeping requirements on undertakers in relation to items of apparatus belonging to them. For example, section 79(1) requires an undertaker, as soon as reasonably practicable after specific events occur, to record the location of every item of apparatus, including the nature of the apparatus (if known) and whether it is for the time being in use.

469 Subsection (3)(c) of this clause inserts a new subsection (1B) into section 79 of the 1991 Act. This new subsection imposes a duty on undertakers to record other information beyond that they are already required to record under section 79(1). This new subsection also makes clear that this duty must be complied with as soon as reasonably practicable after certain events occur, such as placing of an item of apparatus in a street, repairing an item of apparatus or receiving information relating to an item of apparatus under section 80(2)(a), as discussed below.

470 Currently, undertakers are required to make their records, containing information about apparatus, "available for inspection" by others pursuant to the requirement set out in section 79(3) of the 1991 Act. Once these new provisions relating to NUAR are in force, this will no longer be necessary. For example, if a person who wishes to undertake works in the street needs to know what apparatus may lie underground, instead of seeking information from multiple different owners of apparatus (each of whom must currently make that information available under section 79(3)), they will be able to access all of this information directly from NUAR. As discussed elsewhere in these notes, new duties will be placed on undertakers to enter information into NUAR, instead of being required to make information available under section 79(3). In light of this, subsection (3)(d) removes the requirement in section 79(3).

471 Many of these new provisions relating to NUAR deal with how the register will be populated with information, and how the register will operate, in the future. Subsection (3)(f) of this clause inserts a new subsection (3B) into section 79 of the 1991 Act which requires an undertaker, when recording or updating information as required by section 79(1) or new section 79(1B) of that Act, to then enter the recorded or updated information into NUAR within a time period as set out by the Secretary of State in regulations.

472 The existing provisions in section 79, and those inserted by this clause, confer powers to "prescribe" certain matters. Subsection (3)(h) of this clause inserts a new subsection (7) into section 79 of the 1991 Act, providing for this to generally mean, in this section, "prescribed by the Secretary of State". However, in section 79(1) and (2), where (in relation to Wales) existing functions to prescribe matters are already conferred on the Welsh Ministers, provision is made by new subsection (7)(a) so that such matters can be prescribed by the Secretary of State in relation to apparatus in streets in England, and can be prescribed by the Secretary of State or the Welsh Ministers in relation to apparatus in streets in Wales.

473 Before making any regulations under section 79 (as amended by this clause) the Secretary of State must consult the Welsh Ministers, as provided for by new subsection (8) inserted into section 79.

474 Subsection (4) of this clause replaces the existing (and not yet in force) section 80 in the 1991 Act with a new section 80. This new section 80 addresses the scenario where a relevant person is executing works of any description in a street and finds an item of apparatus that does not belong to them.

475 More specifically, subsection (2) of the new section 80 applies when a person with access to NUAR (pursuant to regulations under section 106C(1)) finds an item of apparatus in relation to which prescribed information is either not entered in NUAR or where such information is entered incorrectly. In those circumstances the person must attempt to inform the undertaker who owns the apparatus. The undertaker will then be required, in line with the requirement in section 79(1)(c) of the 1991 Act (as amended by subsection (3)(b) of this clause) to update their own records. Updating their own records in this way will then trigger the requirement in new section 79(3C) for the undertaker to enter this new or updated information into NUAR. If the person is not able to identify the asset owner then they must enter the information into NUAR themselves.

476 A person who fails to comply with subsection (2) of the new section 80 commits a criminal offence, which is triable summarily and, if convicted, can result in a fine not exceeding level 4 on the standard scale.

477 The provisions in the new section 80 confer powers on the Secretary of State to prescribe certain matters through the making of regulations. A number of consultation requirements apply before regulations can be made under this new section, as set out in subsection (5). The Secretary of State must consult representatives of persons likely to be affected by the regulations and such other persons as the person making the regulations considers appropriate. The Secretary of State must also consult the Welsh Ministers.

478 As originally drafted, section 104 of the 1991 Act makes general provision in relation to regulations made under Part 3 of that Act. Subsection (6) of this clause makes a number of amendments to section 104 as a result of the approach this Bill takes to sections 79 and 80 of the 1991 Act. Subsection (6)(b) inserts a new subsection (1A) into section 104, providing that regulations under Part 3 may make different provision for different cases, and supplementary or incidental provision. It also confirms that regulations made under Part 3 shall be made by statutory instrument, and that the negative procedure shall apply in relation to any such regulations made by the Secretary of State.

Clause 58: National Underground Asset Register: Northern Ireland

479 Paragraphs 430-478 of these explanatory notes set out how the NUAR service will operate in England and Wales as a result of clauses 56, 57, 60 and Schedule 1 of the Bill. These provisions allow for a single, sustainable service to operate effectively across England and Wales.

480 NUAR will also operate across Northern Ireland as provided for by clauses 58, 59, 60 and Schedule 2 of the Bill. These clauses (and the Schedule) essentially mirror, for Northern Ireland, the provision made for England and Wales.

481 As set out above, provision for NUAR in England and Wales is made through amendments to the New Roads and Street Works Act 1991. The equivalent legislation for Northern Ireland is the Street Works (Northern Ireland) Order 1995, which this clause amends in order to make equivalent provision for NUAR in Northern Ireland.

482 Subsection (3) of clause 58 inserts new Articles 45A – 45H into the 1995 Order, making equivalent provision to new sections 106A to 106J this Bill inserts into the 1991 Act for England and Wales. These new Articles therefore set out, for Northern Ireland, a legislative framework for NUAR, including empowering the Secretary of State to make provision by regulations in connection with the making of information kept in NUAR available to others, the payment of fees by undertakers in relation to NUAR, requiring undertakers to provide information to the Secretary of State for the purposes of regulations, monetary penalties and arrangements for third parties to exercise relevant functions of the Secretary of State.

Section 45A: National Underground Asset Register

483 New Article 45A in the 1995 Order is, for Northern Ireland, the equivalent of section 106A in the 1991 Act for England and Wales (see paragraph (432) above). This Article places a duty on the Secretary of State to keep a register of information ("NUAR") relating to apparatus in streets in Northern Ireland.

484 Although the legislative requirements to keep a register in England and Wales, and in Northern Ireland, are distinct, the intention is for there to be a single register across all three of these parts of the UK. New Article 45A(5) makes provision to facilitate this.

Section 45B Initial upload of information into NUAR

485 New Article 45B in the 1995 Order is, for Northern Ireland, the equivalent of section 106B in the 1991 Act for England and Wales (see paragraph (436) above). This Article will operate in an equivalent way to the Section 106B in requiring undertakers having apparatus in a street to complete a one-off initial upload of their existing records into NUAR within a time period to be set out by the Secretary of State in regulations.

Section 45C Access to information kept in NUAR

486 New Article 45C in the 1995 Order is, for Northern Ireland, the equivalent of section 106C in the 1991 Act for England and Wales (see paragraph (441) above). This Article makes equivalent provision to allow the Secretary of State to make regulations to allow information kept in NUAR to be made available to others.

Section 45D Fees payable by undertakers in relation to NUAR

487 New Article 45D in the 1995 Order is, for Northern Ireland, the equivalent of section 106D in the 1991 Act for England and Wales (see paragraph (445) above). As in England and Wales the intention is for NUAR to be funded by undertakers having apparatus in a street, that is, those who benefit most from the service. These provisions allow for a fees scheme to be put in place,

providing funding for the operation of NUAR. For these purposes, and as provided for by new Article 45D(7), the income received through such fees, and the expenses incurred in running NUAR, will both be combined across England, Wales and Northern Ireland as the Secretary of State seeks to ensure that – so far as possible and taking one year with another – the fees being imposed match the overall costs of running NUAR.

Article 45E: Providing information for purposes of regulations under Article 45D

488 New Article 45E in the 1995 Order is, for Northern Ireland, the equivalent of section 106E in the 1991 Act for England and Wales (see paragraphs (451) above). In developing and then operating the fees scheme described above, it is likely that the Secretary of State will need to consider a range of different types of information. New Article 45E enables the Secretary of State to impose legally binding requirements on undertakers to provide such information for either or both of the purposes set out in subsection (1).

Article 45F: Monetary Penalties

489 This section gives effect to the new Schedule 2ZA to the 1995 Order (found at Schedule 2 to the Bill) which is, for Northern Ireland, the equivalent of the new Schedule 5A to the 1991 Act (found at Schedule 1 to the Bill) for England and Wales (see paragraph (455) above). Schedule 2ZA makes provision for the Secretary of State to impose monetary penalties as a means of enforcing any requirements to pay fees, or provide information, as set out in regulations made under new sections 45D(1), 45E(1) or 45E(2).

Article 45G: Arrangement for third party to exercise functions

490 New Article 45G in the 1995 Order is, for Northern Ireland, the equivalent of section 106G in the 1991 Act for England and Wales (see paragraph (456) above).

491 The new Articles 45A to 45H and Schedule 2ZA (which will be defined by the amended article 2 of the 1995 Order as the "NUAR provisions") confer a range of functions on the Secretary of State. A number of these functions concern operational aspects of running NUAR, such as the keeping of the register, making information kept in the register available to others, and the receiving of fees. Article 45G makes provision for the approach, as in England and Wales, whereby the Secretary of State can enter into arrangements for another person to exercise these functions of the Secretary of State, save for those set out in Article 45G(7)(a) and (b).

Article 45H: Data Protection

492 New Article 45H in the 1995 Order is, for Northern Ireland, the equivalent of section 106H in the 1991 Act for England and Wales (see paragraph (461) above).

493 It is not anticipated that information processed for the purposes of NUAR will typically include personal data. However, should any processing of personal data take place as a result of the provision made by (or in regulations under) a NUAR provision, section 45H makes clear that this processing will have to be undertaken in accordance with the existing data protection legislation. In this context, "processing", "personal data" and "the data protection legislation" have the same meaning as in the DPA 2018.

494 Subsection (4) of clause 58 makes a number of amendments to article 59 of the 1995 Order, setting out a number of procedural requirements that will apply in relation to regulations made under a NUAR provision. New Article 59(A1) imposes on obligation on the Secretary of State to consult the Department for Infrastructure and the Welsh Ministers before making such regulations. Other new paragraphs inserted into Article 59 – among other things – set out

the relevant Parliamentary procedures which apply to such regulations when made by the Secretary of State.

Clause 59: Information in relation to apparatus: Northern Ireland

495 Clause 59 amends Article 39 of the 1995 Order to make equivalent changes to those made to section 79 of the 1991 Act by clause 57 (see paragraph (467) above).

496 Clause 59(3)(c) inserts a new paragraph (1B) into Article 39, which makes equivalent provision to the new subsection (1B) inserted into section 79 of the 1991 Act. This introduces a requirement for undertakers having apparatus in a street to record additional, prescribed information as soon as practicable after specific events occur. Clause 59(3)(f) inserts new paragraphs (3B) and (3C) into Article 39, requiring this information to be uploaded to NUAR in a prescribed form and manner within a prescribed period.

497 Similarly, as with section 79(3) of the 1991 Act, the requirement for undertakers to make their records "available for inspection" by others at Article 39(3), is removed (see clause 59(3)(d)).

498 Article 40 of the 1995 Order (which is not yet in force) makes equivalent provision to the existing section 80 of the 1991 Act (which is also not yet in force). Clause 59(4) substitutes a new Article 40 into the 1995 Order. The new Article 40, like the new section 80 substituted into the 1991 Act, addresses the scenario where a relevant person is executing works of any description in a street and finds an item of apparatus that does not belong to them.

499 A person who fails to comply with paragraph (2) of the new Article 40, as with the equivalent provisions in the new section 80 inserted into the 1991 Act, commits a criminal offence, which is triable summarily and, if convicted, can result in a fine not exceeding level 4 on the standard scale.

500 The provisions in the new Article 40 confer powers on the Secretary of State to prescribe certain matters through the making of regulations. A number of consultation requirements apply before regulations can be made under this new Article, as set out in paragraph (5). The Secretary of State must consult representatives of persons likely to be affected by the regulations and such other persons as the person making the regulations considers appropriate. The Secretary of State must also consult the Department for Infrastructure.

Clause 60: Pre-commencement consultation

501 This clause makes express provision confirming that any requirement to consult as set out in any provision inserted into the 1991 Act by clauses 56 or 57, or inserted into the 1995 Order by clauses 58 or 59, can be satisfied by consultation before the day on which this Act is passed.

Part 4: Registers of births and deaths

Clause 61: Form in which registers of births and deaths are to be kept

502 Clause 61 amends the Births and Deaths Registration Act 1953 (the BDRA). Subsection (2) 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).

503 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.

504 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.

505 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.

506 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.

507 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.

508 Subsections (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.

509 Subsection (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 64.

Clause 62: Provision of equipment and facilities by local authorities

510 Clause 62 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 63: Requirements to sign register

511 Clause 63 makes further amendments to the BDRA.

512 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;

513 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.

514 New section 38B(3) clarifies that in this section "specified" means specified in regulations under this section.

515 Subsection (3) of clause 63 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 64: Treatment of existing registers and records

516 Subsection (1) of clause 64 specifies that the repeal of section 28 of the BDRA by subsection (3)(c) of this clause 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.

517 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.

518 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.

519 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 61 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.

520 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 61 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 61 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.

521 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 61 comes into force.

Clause 65: Minor and consequential amendments

522 Clause 65 brings Schedule 11 into effect.

Part 5: Data Protection and Privacy

Chapter 1: Data Protection

Terms used in this Chapter

Clause 66: The 2018 Act and the UK GDPR

523 Clause 66 is self-explanatory in explaining the meaning of references to "the 2018 Act" and "the UK GDPR" in chapter 1 of Part 5 of the Bill.

Definitions in the UK GDPR and the 2018 Act

Clause 67: Meaning of research and statistical purposes

524 Clause 67 amends Article 4 of the UK GDPR. Subsection (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.

525 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.

526 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.

527 Clause 67 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.

528 This clause 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 68: Consent to processing for the purposes of scientific research

529 Clause 68 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 68 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 69: Consent to law enforcement processing

530 Clause 69 introduces a definition of consent into Part 3 of the DPA 2018 mirroring the definition under the UK GDPR.

531 Consent should only be used as the grounds for processing where it would be inappropriate to use one of the law enforcement purposes. For example, where a police officer takes fingerprints from the victim of a burglary in order to eliminate their prints from any found at the crime scene. Clearly it would be inappropriate, in this case, to insist that the victim provide them; it should be voluntary.

532 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.

533 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.

534 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.

535 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 70: Lawfulness of processing

536 Clause 70 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).

537 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 DPA 2018 and regulation 41(7) of 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.

538 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 the purposes of a recognised legitimate interest.

539 Subsection (2)(c) prevents new Article 6(1)(ea) of the UK GDPR 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) of the UK GDPR.

540 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.

541 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 (10) 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, and the fact that children (where relevant) may be less aware of the risks and consequences associated with processing of personal data and of their rights in relation to such processing. The Secretary of State can only add a new processing activity to Annex 1 if it is necessary to safeguard a public objective listed in Article 23(1)(c) to (j) of UK GDPR. The regulations must be made by statutory instrument and are subject to the affirmative procedure.

542 New Article 6(11) 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 (11) 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. New Article 6(12) defines the meaning of "intra-group transmission" and "security of network and information systems", expressions used in subsection (11)

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

544 Subsection 6 introduces Schedule 4, which inserts new Annex 1 into the UK GDPR. New Annex 1 to the UK GDPR lists those processing activities that will be regarded as 'recognised legitimate interests' for the purposes of the new lawful ground in Article 6(1)(ea).

545 Subsection 7 removes the words "the controller's" from section 8 of the DPA 2018 to improve the clarity of that provision.

546 Subsections 8 and 9 set out minor and consequential amendments that are needed because of the creation of the new lawful ground in Article 6(1)(ea).

Clause 71: The purpose limitation

547 Clause 71 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.

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

549 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.

550 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.

551 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.

552 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.

553 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.

554 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 compatible through Article 8A(2) 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)).

555 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. 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).

556 Subsection (6) of clause 71 introduces Schedule 5.

557 Subsections (7)-(9) make amendments equivalent to those made to Article 5(1)(b) UK GDPR by clause 71 (2) to sections 36(1) and 87(1) of the DPA 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.

558 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 DPA 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 5.

Clause 72: Processing in reliance on relevant international law

559 Under the UK GDPR, the processing of personal data on grounds of public interest under Articles 6(1)(e) and 9(2)(g) is only lawful if the basis of the processing is set out in "domestic law". Similarly, any processing of personal data relating to criminal offences under Article 10 or under the new exemptions to purpose limitation principle in new Article 8A(3)(e) (inserted by clause 71 of this Bill) must be authorised by domestic law.

560 Subsections (1) to (6) of clause 72 amend these provisions in the UK GDPR to make it clear that relevant international law can also provide the basis for this processing.

561 Subsection (7) inserts new section 9A into the DPA 2018 which provides that the requirement for a basis in or authorisation by relevant international law is met if the processing meets a condition in new Schedule A1 to the DPA 2018.

562 The new Schedule A1 lists as a condition that processing is necessary to respond to a request in accordance with the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime.

563 Subsection (7) also provides the Secretary of State with powers to add other conditions relating to international treaties to the new Schedule and amend or vary conditions via regulations, which are subject to the affirmative resolution procedure. The power also allows the addition of safeguards to such processing, which could include duties on controllers or processors to have specific policies or procedures in place or to retain or provide information about the processing.

Processing of special categories of personal data

Clause 73: Elected representatives responding to requests

564 Clause 73 amends para 23 of Schedule 1 to the DPA 2018, which permits elected representatives to process special category data when acting on behalf of individuals in connection with their casework functions. Elected representatives can currently rely on this exemption for up to four days after an election, but this clause extends that period to 30 days.

Clause 74: Processing of special categories of personal data

565 Article 9(1) of the UK GDPR sets out an exhaustive list of special categories of personal data, sometimes known as "sensitive data". Processing of data in this list is prohibited unless a condition in Article 9(2) is met, together with any associated DPA 2018 Schedule 1 conditions where required. Processing of data in this list is also subject to various obligations or considerations imposed by other provisions in the data protection framework, for example the requirement in Article 37 to designate a data protection officer if certain conditions are met.

566 This clause confers regulation-making powers to the Secretary of State to add new special categories of data, tailor the conditions applicable to their use, and add new definitions, if necessary, to enable the Government to rapidly respond to future technological and societal developments.

567 This clause provides four regulation-making powers to update the protections in Article 9 and reciprocal provisions in Part 3 and Part 4 of the DPA).

568 Clause 74(1) creates a new Article 11A (1) to confer regulation-making powers to the Secretary of State. The powers will enable the Secretary of State, by regulations, to:

- add new special categories of data to the general prohibition in Article 9(1) UK GDPR. Categories in Article 9(1) may not be processed unless the controller meets a condition in Article 9(2), as supplemented by Schedule 1. This power is set out in new Article 11A(1)(a).

- remove any categories of special category data that have been added by such regulations. This power cannot be used to remove any of the pre-existing categories in Article 9(1). This power is set out in new Article 11A(1)(b).

- to make provision that any of the existing conditions in Article 9(2) may or may not be relied on in relation to any new category added by regulations. This is because the conditions under Article 9(2) were drafted with only the current special categories in Article 9(1) in mind. If a new special category is recognised in the future, it may be necessary to alter which of the existing conditions apply to it in order to provide more specific protection. This power is set out in new Article 11A(1)(c).

- to make provision to vary any of the existing conditions in Article 9(2) but only as it relates to any new categories added by regulations. This power cannot be used to remove or vary conditions for existing special categories under Article 9(2). This power is set out in new Article 11A(1)(d).

569 New Article 11A (2) clarifies that the regulation-making powers to remove prohibitions from Article 9(1) and to vary the applicability of conditions under Article 9(2) only apply to new descriptions of special categories added under regulations. The powers cannot be used to remove existing special categories from Article 9(1) or to remove or vary conditions for existing special categories under Article 9(2).

570 New Article 11A (3) supplements these provisions, enabling textual amendments to be made to sections 5, 205, and 206 of the DPA, by making a consequential amendment relying on Article 91A(4b). These provisions contain definitions that may need amending if new descriptions of processing are added in the future to the list of special categories of data in Article 9(1).

571 New Article 11A (4) provides that the regulations made under these powers are subject to the affirmative resolution procedure

572 New Sections 42A and 91A deal with equivalent powers under Part 3 and Part 4 DPA respectively. Section 35(6) of Part 3 DPA sets out a list of "sensitive processing", where the processing described is only lawful where a condition in Schedule 8 DPA can be met, if the data subject has not consented to the processing. Section 86(7) DPA sets out an equivalent list for Part 4. All processing under Part 4 requires a condition under Schedule 9 to be met, and for sensitive processing a condition under Schedule 10 must also be met.

573 New Section 42A provides powers for the Secretary of State to, by regulations:

- Add additional categories of sensitive processing to those provided in section 35(6);

- Remove categories of sensitive processing which have been added under that power;
- Make provision that any of the existing conditions required for sensitive processing under Schedule 8 may or may not be relied upon for added categories of sensitive processing; and
- Make provision to vary conditions under Schedule 8 for categories of sensitive processing added under this power.

574 New section 42A (2) clarifies that the regulation making powers to remove categories of sensitive processing under section 35(6) and vary conditions under Schedule 8 can only be exercised in relation to new categories added by regulations. These powers cannot remove existing categories of sensitive processing under section 35(6) or vary conditions in Schedule 8 in relation to those existing categories.

575 New section 91A provides the same powers for the sensitive processing regime under Part 4 of the DPA. New section 91A provides power to the Secretary of State to, by regulations:

- Add additional categories of sensitive processing to those already provided in section 86(7);
- Remove categories of sensitive processing that have been added under that power;
- Make provision that any of the existing conditions required for sensitive processing under Schedule 10 may or may not be relied upon for added categories of sensitive processing; and
- Make provision to vary conditions under Schedule 10 for categories of sensitive processing added under this power.

576 New section 91A (2) clarifies that the regulation making powers to remove categories of sensitive processing under section 86(7) and vary conditions under Schedule 10 can only be exercised in relation to new categories added by regulations. The powers cannot remove existing categories of sensitive processing under section 86(7) or vary conditions in Schedule 10 in relation to those existing categories.

577 New section 42A(3) and 91A(3) enable amendments to be made to sections 205 and 206 DPA. This will allow definitions to be amended if new categories of sensitive processing are added in the future to the categories already provided in sections 35(6) or 86(7).

578 New sections 42A(4) and 91A(4) provide that regulations made under these powers are subject to the affirmative procedure.

579 Subsections (4) and (7) of this clause amend sections 35(6)(b) and 86(3)(b) DPA to allow the Secretary of State to vary conditions required to be met for sensitive processing in Schedule 8 and Schedule 10 respectively, where those conditions have been added by regulations made under sections 35(6)(a) and 86(3)(a) respectively.

580 The clause also makes consequential amendments to section 202 Investigatory Powers Act 2016 (IPA). Subsection (11) of the clause aligns the language regarding sensitive personal data in section 202 IPA with Part 4 DPA. This clarifies that the existing definition of "sensitive

personal data" in section 202(4) IPA corresponds to the processing to be undertaken and the specified categories of "sensitive processing" in section 86(7) DPA.

581 Lastly, new section 202A IPA enables the Secretary of State to, by regulations, add categories of sensitive processing described in Part 4 DPA to section 202(4) IPA. This is to allow for changes made to the descriptions of sensitive processing contained in section 86(7) to be included in s.202(4) IPA 2016 where appropriate but does not confer powers to remove or amend existing categories referred to in section 202(4) IPA. Regulations under this power are subject to the affirmative procedure.

Data subject's rights

Clause 75: Fees and reasons for responses to data subjects' requests about law enforcement processing

582 Clause 75 introduces new subsection 4A into section 53 of the DPA 2018. Section 53(1) currently provides controllers operating under Part 3 of the DPA 2018 the option to refuse to respond to, or charge a reasonable fee for responding to, requests from data subjects which are determined to be manifestly unfounded or excessive. New subsection 4A will provide the Secretary of State with a regulation making power to require controllers to publish guidance on the fees they charge for responding to such requests. This mirrors the current power available for general processing under section 12(2) of the DPA 2018.

583 Clause 75 also introduces new subsections (6) and (7) in section 53. These new subsections clarify that, when refusing to respond to a data subject request that is manifestly unfounded or excessive, controllers must inform the data subject of the refusal and the data subject's right to complain to the Information Commissioner. They also confirm that this notification must happen without undue delay.

Clause 76: Time limits for responding to data subjects' requests

584 Clause 76 changes the time limits for responding to requests from data subjects. Subsection (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.

585 In general, requests from data subjects must be responded to within one month of being received. New Article 12A and (2) UK GDPR clarify the circumstances where this response time is different and what the time period is instead.

586 New Article 12A sets out that an extension may be necessary due to the number of requests submitted in relation to the data subject. New Article 12A (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.

587 New Article 12A(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.

588 Subsection (5) of clause 76 amends section 45 of Part 3 DPA 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, such 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).

589 Subsection (6) amends section 54 DPA 2018 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. New subsection (3A) replicates the provision in new Article 12A(3) UK GDPR 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).

590 New subsections (3C) and (3D) of section 54 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 new Article 12A(5) for a controller to be able to pause the response time if further information is required in order to proceed.

591 Subsection (7) of clause 76 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 subsection (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 77: Information to be provided to data subjects

592 Clause 77 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, when collected directly from the data subject (Article 13) or within a reasonable period (at the latest within one month) after obtaining the personal data, for personal data obtained indirectly (Article 14).

593 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 77(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 85.

594 New paragraph 6 of Article 13 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.

595 New paragraph 7 of Article 13 outlines that any controller relying on the new paragraph 5 must take appropriate measures to protect the data subject's rights, freedoms and legitimate interests, including by making the information publicly available that would otherwise be provided to the data subject through Article 13. For example, if it is considered

disproportionate for a controller to issue individual notices, the information normally required to be provided as part of Article 13 requirements (such as identity and contact details of the data protection officer if applicable) should be made publicly available so that a data subject has this information if they wish to search for it. Subsection (2) of clause 11 also amends Article 14 of the UK GDPR. Clause 77 (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 Article 14 but are made to accommodate other changes to Article 14 made by clause 77.

596 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 subsection (2) of this clause, 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.

597 Subsection (2)(b) of clause 11 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.

598 Paragraph 7 of Article 14 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 subsection (2)(a)(ii) of this clause

Clause 78: Searches in response to data subjects' requests

599 Clause 78 amends the provisions in the UK GDPR and DPA 2018 which set out the right of access to information and personal data across the United Kingdom's data protection regime to clarify that controllers only have to carry out reasonable and proportionate searches for information and personal data requested. This codifies the principle currently set out in domestic case law.

600 Subsection (5) stipulates that this amendment should be treated as coming into force on 1st January 2024.

Clause 79: Data subjects' rights to information: legal professional privilege exemption

601 Clause 79 inserts a new section 45A into the DPA 2018 which mirrors the current exemption for material which is subject to legal professional privilege or, in Scotland, to confidentiality of communications under the UK GDPR. Legal professional privilege protects all communications between a professional legal advisor and their clients.

602 Sub-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 80: Automated decision-making

603 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.

604 Clause 80 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.

605 Article 22A(1)(a) clarifies it is necessary for a decision based on solely automated processing to be 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.

606 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.

607 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 the processing of their personal data in this way. The second condition, as an alternative, has two requirements:

a. The first requirement is that such activity:

i. is necessary for entering into, or the performance of, a contract between a data subject and controller; or

ii. is required or authorised by law.

b. The second requirement is that the activity also satisfies Article 9(2)(g); that is, the activity must be necessary for reasons of substantial public interest.

608 Article 22B(4) prohibits reliance on new Article 6(1)(ea) when taking significant decisions based solely on automated processing.

609 Article 22C(1) and C(2) set out the safeguards for automated decision making for significant decisions based either entirely or partly on personal data and solely on automated processing. The safeguards replace the provisions at Article 22(3) and Article 22(3A) of the UK GDPR and section 14 of the DPA 2018. The clause requires controllers to ensure that the relevant safeguards are in place for data subjects. These safeguards include the requirement on controllers to provide information to data subjects about significant decisions being taken through solely automated processing, the right to contest those decisions, and the right to seek human intervention at the request of the data subject.

610 Article 22D(1) and D(2), confers regulation making powers to the Secretary of State, through secondary legislation, to provide that for the purposes of:

- Article 22A(1)(a) to describe those cases that are, or are not, to be taken to have meaningful human involvement and;
- Article 22A(1)(b)(ii) to describe what is, or is not, to be taken as a significant decision.

611 These powers will allow the Secretary of State to determine when meaningful involvement can be said to have taken place in light of constantly emerging technologies, as well as

changing societal expectations of what constitutes a significant decision in a data protection context.

612 Article 22D(3) confers a regulation making power on the Secretary of State to add new provisions relating to the safeguards required by new Article 22C(2); to include measures in addition to those described by Article 22C(2); to impose requirements which supplement Article 22C(2) and to specify measures which are not to be taken to satisfy points (a) to (d) of Article 22C(2). Article 22D(4) provides that regulations made under paragraph 4 may not amend Article 22C. As new technologies emerge, these powers enable the Government to provide legal clarity on the circumstances in which safeguards must apply to ensure individuals are protected and have access to safeguards.

613 Subsection (3) of clause 80 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. With some exceptions, these new sections broadly mirror the approach taken under Articles 22A – D of the UKGDPR. These notes highlight where the Government has taken a different approach between the two regimes.

614 Unlike Article 22A, section 50A(1)(b)(i) and (ii) restricts a significant decision to those that produces an **adverse** legal or similarly significant effect on a data subject rather than all such decisions. This is because under Part 3, data subjects are unlikely to perceive the majority of decisions taken by competent authorities as positive, whereas the effect of a significant decision under the UK GDPR may be more nuanced.

615 Section 50B restricts taking significant decisions based entirely or partly on the processing of sensitive personal data (the equivalent of special categories of data under the UK GDPR), solely via automated processing, to situations where either the data subject has given their consent or the processing is required or 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 taking such a decision. This is because it is not considered likely that such a situation would ever arise under Part 3.

616 Section 50C(1) and (2)mirror the list of safeguards available to data subjects under article 22C(1) and (2).

617 Section 50C(3) provides an exemption to the requirement to apply the safeguards provided that:

- it is required for one of the reasons set out under section 50C(4), such as to avoid obstructing an inquiry or, to protect national security;
- the controller reconsiders the decision and this is carried out as soon as is reasonably practicable; and
- the reconsideration of the decision includes meaningful human involvement.

618 Section 50D mirrors the powers of the Secretary of State to make further provisions about automated decision-making set out under Article 22D.

619 Subsections (4) and (5) of clause 14 make 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.

Logging of law enforcement processing

Clause 81: Logging of law enforcement processing

620 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.

621 The purposes for which these logs may be used are set out in subsection (4). One key purpose is self-monitoring, including for the purpose of conducting internal disciplinary hearings. This may, for example, arise where an officer or member of police staff is suspected of inappropriately accessing a police record. The logs of consultation and disclosure must record, as far as possible, the identity of the person consulting or disclosing the personal data and the recipients of the personal data. It must also record, the date and time the personal data was consulted, or disclosed, and the justification for doing so.

622 Clause 81 removes the requirement for a competent authority to record a 'justification' in the logs when consulting or disclosing personal data. This is because it is unlikely that a person accessing records inappropriately would record an honest justification. It is also because it is technologically challenging for systems to automatically record it.

Codes of conduct

Clause 82: General processing and codes of conduct

623 Clause 82 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 114.

Clause 83: Law enforcement processing and codes of conduct

624 Clause 83 inserts new section 71A into the DPA 2018 which enables expert public bodies, who have sufficient knowledge and experience, to create codes of conduct, mirroring the existing provision under the UK GDPR. These are tailored, sector-specific, pieces of guidance which are signed off by the Information Commissioner. 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.

625 Law enforcement agencies are expected to monitor their compliance with any code of conduct produced under the law enforcement processing regime through existing internal auditing mechanisms.

International transfers of personal data

Clause 84: Transfers of personal data to third countries and international organisations

626 Clause 84 inserts Schedules 7, 8 and 9, 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 85: Safeguards for processing for research etc purposes

627 Clause 85 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 85 (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.

628 Subsection (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 85 (2) also replicates the definition of "approved medical research" from section 19 of the DPA 2018. The Secretary of State may, by regulations, make further provisions about when the requirement for appropriate safeguards under Article 84B(2) is, or is not, satisfied. This power can only be used to add a paragraph to Article 84C and vary or omit any paragraphs added by regulations. Regulations under this Article may not amend or revoke Article 84C(2)- (4) but may change the meaning of "approved medical research" for the purposes of Article 84C. Regulations under this Article are subject to the affirmative resolution procedure.

Clause 86: Section 85: consequential provision

629 Clause 86 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 86which 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 87: National Security Exemption

630 Clause 87 inserts a new section 78A into Part 3 of the DPA 2018, which provides an exemption from certain provisions of Part 3, 5, 6 & 7 where this is required for the purposes of safeguarding national security. The provisions that may be disapplied in such circumstances are listed in subsection (2) and includes the majority of the data protection principles, the rights of the data subject, certain obligations on competent authorities and processors, and various enforcement provisions.

631 Part 3 of the DPA 2018 already enables competent authorities to apply exemptions to specified rights where this is necessary to protect national security. However, this clause ensures that they have the same exemptions already available to organisations, such as businesses, who

operate under the UK GDPR (section 26 of the DPA 2018) as well as the intelligence services (section 110 of the DPA 2018).

Intelligence Services

Clause 88: Joint processing by intelligence services and competent authorities

632 Clause 88 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.

633 Subsection (2) amends section 82 of the DPA 2018, which currently applies Part 4 only 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.

634 Subsection (3) of clause 88 inserts new sections, 82A – 82E, that impose the conditions for designation notices.

635 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.

636 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.

637 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.

638 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.

639 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.

640 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.

641 82E allows a designation notice to be appealed to the tribunal if a person is directly affected by the notice.

Clause 89: Joint processing: consequential amendments

642 Subsections (2)–(8) of clause 89 makes necessary consequential amendments to the DPA 2018 to reflect the changes made by clause 88, 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 90: Duties of the Commissioner in carrying out functions

643 Clause 90 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.

644 Subsection (2) 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.

645 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.

646 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. There is also a new duty to have regard to the fact that children may be less aware of the risks and consequences associated with processing of personal data and of their rights in relation to such processing.

647 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.

648 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).

649 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.

650 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.

651 Subsection (4) of clause 90 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.

652 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 91: Codes of practice for the processing of personal data

653 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 that 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.

654 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.

655 Clause 91 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.

656 To enable this in a structured and methodical manner, section 128 (Other codes of practice) will be 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.

657 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.

658 Subsections (3) to (9) of clause 91 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 92: Codes of practice: panels and impact assessments

659 Clause 92 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.

660 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.

661 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.

662 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.

663 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.

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

665 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.

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

667 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.

668 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.

669 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.

670 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 93: Manifestly unfounded or excessive requests to the Commissioner

671 Clause 93 amends the DPA 18 to clarify that, when a request is made to the Commissioner to which the Commissioner is required or authorised to respond under the data protection legislation (for example, because it relates to their tasks, duties and functions), the Commissioner may charge a reasonable fee or refuse a request where a request is manifestly unfounded or excessive.

672 This clause amends section 135 of the DPA 18 to make clear that the Commissioner may refuse to deal with a manifestly unfounded or excessive request made by any person.

673 Sections 134 and 135 of the DPA 18 confer separate powers to charge fees. Where a request is made (whether manifestly unfounded 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), 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.

674 New 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.

675 Clause 93 (2)(f) sets out that this is an exception to the general rule set out in Article 57(3) of the UK GDPR that the performance of tasks should be free of charge for data subjects.

676 Clause 93(3) is self-explanatory: it amends section 136(1) to ensure consistency with the streamlining of provisions (see below).

677 Clause 93(4) omits paragraph 4 from Article 57 of the UK GDPR. This is to streamline legislative provisions, ensuring that provisions related to manifestly unfounded or excessive requests to the Information Commissioner are located in section 135 of the DPA 18.

Clause 94: Analysis of performance

678 Clause 94 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 Commissioner's performance (see section 139A(1) and (3).

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

Clause 95: Notices from the Commissioner

680 Subsection (2) of clause 95 omits section 141 (Notices from the Commissioner) of the DPA 2018, and subsection (3) inserts new section 141A (Notices from the Commissioner) instead.

681 New section 141A(2) sets out the four ways in which a notice can be given to a person (referred to here as "recipient") by the Commissioner under the DPA 2018.

682 Subsection (3) of new section 141A then defines the term "relevant individual" for the purposes of giving a notice by hand under subsection (2)(a). For example, when giving the notice to a body corporate (excluding partnerships), it must be handed to an officer of that body, or when giving it to a partnership it must be given to either a partner in the partnership or a person who has control or management of the partnership business.

683 The term "proper address" for the purposes of leaving a notice or posting it under section 141(A)(2)(b) and (c) is defined in subsections (4) and (5). Subsection (4) provide that the proper address should be one specified by the recipient (or someone acting on their behalf) as an address where they will accept service of notices and other documents, but in the event such an address hasn't been specified then the proper address is to be determined under subsection (5). Subsection (4) is also relevant when considering the application of section 7 of the Interpretation Act 1978 which deals with the service of documents by post.

684 New section 141A(6) of new section 141A expands on the meaning of a recipient's "email address" for the purpose of subsection (2)(d).

685 Subsection (7) of new section 141A confirms that a notice issued by the Commissioner is treated as given 48 hours after it was sent.

686 Subsection (8) of new section 141A expands on the meaning of the term "officer" in relation to a body corporate, this is relevant when the Commissioner hands a notice to a relevant individual defined under subsection (3)(b).

687 New section 141A (9) makes it clear that whilst new section 141A sets out ways in which the Commissioner can serve notices, it does not preclude the Commissioner from giving a notice using any other lawful means.

688 Subsection (4) makes a consequential amendment to Schedule 2 to the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (S.I. 2016/696).

Enforcement

Clause 96: Power of the Commissioner to require documents

689 Clause 96 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.

690 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 97: Power of the Commissioner to require a report

691 Clause 97 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.

692 Subsection (1) is self-explanatory.

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

694 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.

695 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.

696 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.

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

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

699 Clause 97 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.

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

701 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.

702 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.

703 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.

704 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.

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

706 Subsection (4) of clause 97 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.

707 Subsection (5) of clause 97 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 98: Assessment notices: removal of Ofsted restriction

708 Clause 98 removes the Office for Standards in Education, Children's Services and Skills' (Ofsted) exemption to the ICO's assessment notice power under section 147(6)(b) of the DPA 2018. This allows the ICO to audit Ofsted's function as a registration authority in the event of a suspected data breach.

Clause 99: Interview notices

709 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.

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

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

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

713 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).

714 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.

715 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.

716 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.

717 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.

718 Subsection (9) is self-explanatory.

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

720 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.

721 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.

722 Subsection (4) is self-explanatory.

723 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).

724 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.

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

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

727 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.

728 Subsubsection (3) of this provision 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.

729 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.

730 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.

731 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.

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

733 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.

734 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.

735 Subsection (9) is self-explanatory.

736 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).

737 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.

738 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.

739 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 100: Penalty notices

740 Clause 100 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.

741 This clause 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.

742 This clause 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 101: Annual report on regulatory action

743 Clause 101 amends the DPA 2018 by making provision for the Commissioner to annually publish a report detailing how it has discharged its regulatory functions.

744 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.

745 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.

746 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.

747 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.

748 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.

749 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.

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

Clause 102: Complaints by data subjects

751 Clause 102 inserts new sections 164A and 164B into the DPA 2018.

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

753 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.

754 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.

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

756 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.

757 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.

758 New section 164B(1) 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.

759 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.

760 Subsections (3)-(6) streamline provisions relating to complaints by data subjects, by merging relevant articles of the UK GDPR into the DPA 2018. This ensures relevant provisions regarding complaints to the Information Commissioner about infringements of the data protection legislation are located in section 165 of the DPA 2018.

761 Subsection (7) introduces Schedule 10 containing miscellaneous minor and consequential amendments to the UK GDPR and the DPA 2018 relating to complaints by data subjects.

Clause 103: Court procedure in connection with subject access requests

762 Clause 103 inserts new section 180A into the DPA 2018.

763 New section 180A(1) establishes that section 180A applies in court proceedings to determine whether a data subject is entitled to information in response to a subject access request made under any of the UK's data protection regimes.

764 New section 180A(2) sets out that the court can require the controller to provide them with the information in question. The controller must provide any requested information which would fall within scope of the rights as set out in section 180A(1).

765 New section 180A(3) ensures that the court cannot require the information set out in subsection (1) to be disclosed to the data subject by any means until it has been determined that the data subject is entitled to it.

766 New section 180A(4) states that the searches for information controllers must make when required to by the court do not need to go beyond the requirements of a reasonable and proportionate search for information when responding to a subject access request.

767 The purpose of this provision is to ensure that courts in relevant cases may inspect material that has been withheld in response to a subject access request without the material having been disclosed to the data subject, when determining whether or not the material is exempt from disclosure. Similar provision was included in the Data Protection Act 1998 (section 15(2) of that Act). In *X v The Transcription Agency and another [2023] EWHC 1092 (KB)* the High Court rejected an argument that the absence of equivalent provision in the Data Protection 2018

(which repealed and replaced the 1998 Act) indicated that Parliament intended that courts should not be able to inspect the material in the absence of the claimant. New section 180A puts the position beyond doubt.

Clause 104: Consequential amendments to the EITSET Regulations

768 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").

769 Clause 104 amends Schedule 2 of the EITSET Regulations in order to apply (with appropriate modification) the changes made by other provisions in the bill.

770 Amongst amendments made 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.

771 This clause 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.

772 This clause 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 105: Protection of prohibitions, restrictions and data subject's rights

773 Subsections (1) to (5) of clause 105 amend the DPA 2018 by inserting new section 183A, 183B and 186A into the DPA 2018 as well as making amendments to existing section 186. The purpose of these provisions is to ensure there are clearer rules about the relationship between key elements of the data protection legislation and: (i) other provisions in legislation or rules of law relating to the processing of personal data, and (ii) restrictions or prohibitions in legislation on disclosures of personal data. This is needed as a result of the changes to the interpretative effects on EU-derived legislation, such as the UK GDPR and other EU-derived elements of the UK's data protection legislation, made by the EU (Withdrawal) Act 2018 and the Retained EU law (Revocation and Reform) Act 2023.

774 Clause 105 (2) inserts a new section 183A into the DPA 2018.

775 Subsection (1) of new section 183A sets out a presumption, in relation to any relevant enactments, or any rules of law, conferring powers or imposing duties relating to the processing of personal data, that requirements under the "main data protection legislation" are not override by such powers or duties.

776 The “main data protection legislation”, “relevant enactment” and “requirement” are defined in subsection (4) of new section 183A. Subsection (4) sets out which parts of the data protection legislation constitute the “main data protection legislation” for the purposes of new section 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 section 105 (2) of the Data (Use and Access) Act 2024 comes into force. This means that the presumption in subsection (1) does not apply to legislation passed or made before the day on which new section 183A comes into force. The reference to “enactment” includes devolved legislation (see section 205(1) of the DPA 2018).

777 Subsection (2)(a) of new section 183A ensures that subsection (1) does not apply to any provisions 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 to the extent that the legislation makes express provision to this effect. 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.

778 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 purposes 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).

779 Subsection (5) of new section 183A provides 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.

780 Clause 105(3) amends the DPA 2018 by inserting a new section 183B into the DPA 2018.

781 New section 183B makes provision about the relationship between pre-commencement enactments which impose a duty, or confer a power, to process personal data and the main data protection legislation (see subsection (1)).

782 The "main data protection legislation" and “requirement” are defined in subsection (5)(a) of new section 183B as having the same meaning as in new section 183A. Subsection (5)(b) defines “pre-commencement enactment” for the purposes of subsection (1) as meaning any enactment that has been passed or made before the day on which section 105(2) of the Data (Use and Access) Act 2024 comes into force. This limits the effect of subsection (1) to legislation passed or made before the day on which new section 183A comes into force. The reference to “enactment” includes devolved legislation (see s.205(1) of the DPA 2018).

783 Subsection (2) of new section 183B provides that the relationship described in new section 183B(1) is not changed by the removal of the principal of the supremacy of EU law in section 5(A1) of the European Union (Withdrawal) Act 2018 nor the repeal of section 5(1) to (3) of that Act. These changes to the European Union (Withdrawal) Act 2018 were made by section 3 of the Retained EU Law (Revocation and Reform) Act 2023. This will apply in cases in which the principle of supremacy of EU law was relevant to the relationship before 1 January 2024.

784 Subsection (3) of new section 183B provides that where the relevant provision of the main data protection legislation is a provision of, or made under, the UK GDPR, section 5(A2) of the European Union (Withdrawal) Act 2018 does not apply to the relationship described in subsection (1). Section 5(A2) provides that provisions of assimilated direct legislation are subject to domestic enactments (so far as incompatible with them). The UK GDPR constitutes assimilated direct legislation and therefore falls within the scope of section 5(A2).

785 Subsection (4) of new section 183B states that nothing is to be implied about a relationship described in new section 183B(1) merely due to the fact that express provision with similar effect to section 183A(1) is made in connection with one relationship but not another.

786 Subsection (6) of new section 183B states that section 183A(5) applies for the purposes of subsection (1)(a) of new section 183B in the same manner that it applies for the purposes of section 183A(1). In other words, 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.

787 Clause 105 (4) makes some amendments to section 186 of the DPA 2018 to clarify its intended application and effect, particularly in light of new section 183A and new section 186A. For example, new section 186(2A)(c) reflects new section 183A(2)(b) by providing that the rule in section 186(1) does not apply to the extent that an enactment makes express provision to the contrary referring to section 186 itself or a provision listed in section 186(2). Whether or not devolved legislation is able to make such provision will depend on the terms of the relevant devolution settlement.

788 Clause 105(5) amends the DPA 2018 by inserting a new section 186A into the DPA 2018. New section 186A builds on section 186 DPA 2018 by making further provision in relation to the interaction between the data protection legislation and other existing legislative provisions or rules of law containing prohibitions or restrictions on the disclosure of information or authorising the withholding of information.

789 New section 186A makes provision about the relationship between pre-commencement enactments which prohibit or restrict the disclosure of information or authorise the withholding of information and provisions of the UK GDPR or the DPA 2018 listed in section 186(2) (see subsection (1)).

790 "Pre-commencement enactment" is defined in subsection (5) of new section 186A for the purposes of subsection (1) as meaning any enactment that has been passed or made before the day on which section 105 (4) of the Data (Use and Access) Act 2024 comes into force, other than an enactment contained in, or made under, a provision of the data protection legislation listed in section 186(2) or (3). The reference to "enactment" includes devolved legislation.

791 Subsection (2) of new section 186A provides that the relationship described in subsection (1) is not changed by the removal of the principal of the supremacy of EU law in section 5(A1) of the European Union (Withdrawal) Act 2018 nor the repeal of section 5(1) to (3) of that Act. These changes to the European Union (Withdrawal) Act 2018 were made by section 3 of the Retained EU Law (Revocation and Reform) Act 2023. This will apply in cases in which the principle of supremacy of EU law was relevant to the relationship before 1 January 2024.

792 Subsection (3) of new section 186A provides that in relation to pre-commencement legislation, there may be occasions when an existing express or implied contrary indication means that section 186(1) does not apply.

793 Subsection (4) of new section 186A indicates that no inference should be drawn about the relationship described in new section 186A(1) merely due to the fact that express provision stating that section 186(1) applies is made in connection with one such relationship but not another.

794 Clause 105 (6) inserts a cross-reference to new section 183A and a signpost to new section 183B(3) into section 5(A3)(a) of the European Union (Withdrawal) Act 2018, as inserted by section 3 of the Retained EU Law (Revocation and Reform) Act 2023. Section 5(A3) contains exceptions from the interpretation rule in section 5(A2) of the European Union (Withdrawal) Act 2018, as also inserted by section 3 of the Retained EU Law (Revocation and Reform) Act 2023. That rule says that provisions of assimilated direct legislation (such as the UK GDPR) are subject to domestic enactments (so far as incompatible with them). The amendments have the effect that the rule is disapplied where new section 183A applies.

795 Clause 105 (7) provides that subsections (3), (5) and (6)(c) of section 105 of the Data (Use and Access) Act 2024 are to be treated as having come into force on 1 January 2024. This means that those subsections will be treated as having had effect from the commencement of section 3 of the Retained EU Law (Revocation and Reform) Act 2023.

Miscellaneous

Clause 106: Regulations under the UK GDPR

796 Clause 106 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 107: Further minor provision about data protection

797 Clause 107 introduces Schedule 11 containing miscellaneous minor amendments to the UK GDPR and the DPA 2018.

Chapter 2: Privacy and electronic communications

Clause 108: The PEC Regulations

798 Clause 108 defines "the PEC Regulations" for the purposes of this chapter.

Clause 109: Interpretation of the PEC Regulations

799 Clause 109 amends Regulation 2 of the PEC Regulations.

800 Subsection (2) amends Regulation 2(1) of the PEC Regulations.

801 Subsection (2)(a) makes it clear that that the definition of "call" includes all calls, including those that are attempted irrespective of whether they connect with the intended recipient.

802 Subsection 2(b) 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.

803 Subsection (2)(c) is a technical amendment which inserts the meaning of "direct marketing" into Regulation 2 for ease of reference. The definition is currently drawn from the DPA 2018 (see paragraph 432(6) of Schedule 19 to the DPA 2018). Direct marketing covers all types of advertising, marketing or promotional material. It includes commercial marketing and the promotion of aims and ideals. A neutrally-toned service message that is sent to comply with regulatory requirements (e.g. a bank updating a customer about changes in interest rates) would not usually count as direct marketing, unless parts of the message actively promote or encourage a person to take a particular action. See guidance produced by the Information Commissioner's Office.

804 Subsection (3) of clause 109 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 "recipient" should be taken to mean the 'intended recipient'.

805 Subsection (4) removes the reference to regulation 2(3) of the PEC Regulation which was previously deleted from the regulation.

806 Subsection (5) inserts new paragraphs (5) and (6). New paragraph (5) states that references to periods of time expressed in hours, days, weeks, months or years are to be interpreted in accordance with Article 3 of the Periods of Time Regulation. New paragraph (6) defines the meaning of "the Periods of Time Regulation". This provision ensures consistency with section 205(2) of the DPA 2018 and new Article 4A of the UK GDPR (inserted by paragraph 3 of Schedule 11 to this Bill).

Clause 110: Duty to notify the Commissioner of personal data breach: time periods

807 The PEC Regulations include rules on reporting breaches of personal data to the Information Commissioner for organisations providing electronic communications services to the public (e.g. telecoms providers and internet service providers). These rules are supplemented by provisions in the retained version of the Commission Regulation (EU) No 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications ("Regulation 611/2013").

808 The current effect of regulation 5A of the PEC Regulations and Article 2 of Regulation 611/2013 is that organisations must report personal data breaches to the Information Commissioner no later than 24 hours of becoming aware of the breach. Subsection (1)(a) of clause 110 changes this so that personal data breaches must be reported without undue delay and, where feasible, not later than 72 hours.

809 Subsection (1)(b) inserts a new paragraph 3A into the PEC Regulations stating that where a personal data breach notification (under paragraph 2) is not made within 72 hours, reasons for the delay must be provided.

810 Subsection (2)(a) and (b) refers to the fixed monetary penalty in 5C of the PEC Regulations and clarifies how to calculate the 21 day period under regulation 5C(4)(f) and (5) of the PEC Regulations.

811 Subsection (3) amends Article 2 of Regulation 611/2013 to reflect the new time limits for breach reporting.

812 Subsection (3)(a) amends paragraph 2 of Article 2 of Regulation 611/2013. Subsection (3)(a)(i) amends the first sub-paragraph to state that service providers must report a personal data breach without undue delay and, where feasible, not later than 72 hours of becoming aware of it.

813 Subsection (3)(a)(ii) is a consequential amendment on new paragraph 3 of Article 2.

814 Subsection (3)(a)(iii) inserts a new subparagraph which states that paragraph 2 is to be interpreted in accordance with Article 3 of Regulation (EEC, Euratom) No. 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits. This provision ensures consistency with section 205(2) of the DPA 2018, new Article 4A of the UK GDPR (inserted by paragraph 3 of Schedule 11 to this Bill) and new paragraph (5) of Regulation 2 of the PEC Regulations (inserted by clause 109 to this Bill).

815 Subsection (3)(b) amends paragraph 3 of Article 2 of Regulation 611/2013 to state that where the information (which is requested under Annex 1 of the Regulation) is not available to be included in the personal data breach notification, it may be provided in phases to the Information Commissioner without undue further delay.

Clause 111: Storing information in the terminal equipment of a subscriber or user

816 Clause 111 amends regulation 6 of the PEC Regulations. Subsection (4) introduces Schedule 12 to this Act, which inserts new Schedule A1 to the PEC regulations.

817 Subsection (2) of clause 111 replaces regulation 6 of the PEC Regulations which sets out rules on the circumstances in which a person can store information, or gain access to information stored, in the "terminal equipment" of a subscriber or user. Terminal equipment may include, for example, computers, mobile phones, wearable technology, smart TVs and connected devices, including the Internet of Things.

818 New regulation 6(1) provides that subject to the exceptions in Schedule A1, organisations are prohibited from storing information or gaining access to information stored in the terminal equipment of an individual.

819 New regulation 6(2)(a) clarifies for the purposes of this regulation and new Schedule A1 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.

820 New regulation 6(2)(b) clarifies that a reference 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 Wi-Fi probe requests.

821 Subsection (3) of clause 111 inserts new regulation 6A into the PEC Regulations.

822 New regulation 6A(1)(a) introduces a power for the Secretary of State to add new exceptions to the prohibition in regulation 6(1). The power would also allow the Secretary of State to omit or vary any existing exceptions to the prohibition.

823 Paragraph (1)(b) of new regulation 6A provides that the Secretary of State 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.

824 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".

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

826 Subsection (5) of clause 111 makes it clear how consultation requirements under regulation 6A may be satisfied.

Clause 112: Emergency alerts: interpretation of time periods

827 Clause 112 clarifies how the period of time in regulation 16A(6) of the PEC Regulation should be calculated.

Clause 113: Commissioner's enforcement powers

828 Clause 113 updates the ICO's powers of enforcement in relation to the PEC Regulations, which currently rely on powers in the Data Protection Act 1998. The effect of this provision will be to apply some of the more modern enforcement powers in the DPA 2018 to the PEC Regulations.

829 Subsections (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, subject to the modification in Schedule 13.

830 Subsection 4(a) includes technical amendments to aid the readability of the legislation, including updating "county court" references.

831 Subsection (4)(b) 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".

832 Subsection (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 13.

833 Subsections (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.

834 Under subsection (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 13 which sets out modifications to the enforcement regime in the DPA 2018, so that it can be applied to the PEC Regulations.

835 Subsection (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.

836 Subsection (10) makes it clear how consultation requirements under regulation 5C may be satisfied.

Clause 114: Codes of conduct

837 Clause 114 inserts new regulations 32A, 32B and 32C into the PEC Regulations.

838 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.

839 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.

840 New regulation 32A(3) sets out an illustrative list of the matters that a code of conduct may make provisions regarding.

841 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.

842 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.

843 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

844 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 Commissioner to give an opinion on whether the code complies with the UK GDPR and relevant PEC Regulations or just relevant PEC Regulations.

845 New regulation 32A(9) sets out the meaning of terms used in the regulation.

846 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.

847 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.

848 New regulation 32B(3) requires the Commissioner to publish guidance about how they propose to take decisions about accreditation under this regulation.

849 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.

850 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.

851 New regulation 32B(7) states that in this regulation the term "public body" has the same meaning as in regulation 32A.

852 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.

853 Subsection (3) of clause 114 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.

854 Subsection (4) amends new Schedule 1 to the PEC Regulation which is inserted by Schedule 13 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.

Part 6: The Information Commission

Clause 115: The Information Commission

855 Together, clauses 115, 116, 117, 118 and Schedule 14 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.

856 Clause 115 inserts a new section 114A into the DPA 2018, which establishes the Information Commission. Schedule 14 inserts a new Schedule 12A into the DPA 2018, which makes further provision about the new body.

Clause 116: Abolition of the office of Information Commissioner

857 Clause 116 makes provision for the abolition of the office of Information Commissioner.

858 Subsection (1) abolishes the office of Information Commissioner.

859 Subsections (2)-(7) make amendments to the DPA 2018.

Clause 117: Transfer of functions to the Information Commission

860 Clause 117 makes provision for the transfer of functions from the Information Commissioner to the Information Commission.

861 Subsection (1) transfers the functions of the office of Information Commissioner to the new body corporate, that is the Information Commission.

862 Subsection (2) makes provision for references to the Information Commissioner in enactments or other documents (whenever passed or made) as defined in section 135 of this Act, including this Act, to be treated as references to the Information Commission so far as appropriate in consequence of the transfer of functions under subsection (1).#

Clause 118: Transfer of property etc to the Information Commission

863 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.

864 Subsection (2) sets out the things that may be transferred under any such scheme.

865 Subsection (3) sets out the nature and scope of the transfer scheme.

866 Subsection (4) provides for modifications to be made to the transfer scheme.

867 Subsection (5) explains that references to rights and liabilities in subsection (3) include rights and liabilities relating to a contract of employment.

Part 7: Other provision about use of, or access to, data

Information standards for health and social care

Clause 119: Information standards for health and adult social care in England

868 Clause 119 makes provision about information standards for health and adult social care in England and information technology. It gives effect to Schedule 154 which amends Part 9 of the Health and Social Care Act 2012.

869 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.

Smart meter communication services

Clause 120: Grant of smart meter communication licences

870 Clause 120 introduces Schedule 16 to the Bill, which makes provision in connection with the grant of smart meter communication licences.

Information to improve public service delivery

Clause 121: Disclosure of information to improve public service delivery to undertakings

871 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. Clause 121 amends section 35 to also enable the sharing of information to improve the delivery of public services to businesses.

872 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.

873 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.

874 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.

875 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.

Retention of information by providers of internet services

Clause 122: Retention of information by providers of internet services in connection with death of child

876 Subsection (1) of clause 122 amends the Online Safety Act 2023, to include a provision on the retention of information by internet service providers in cases involving the death of a child.

877 Subsection (2) removes the signpost in s.100(7) of the Online Safety Act to s.103 of that Act and inserts new subsection 8(A) after subsection 8. Subsection 8(A) confirms that an information notice issued under s.100(1) must not require or authorise processing of information which could contravene the data protection legislation (as defined in s.236(1) of the Online Safety Act).

878 Subsection (3)(a) amends s.101 of the Online Safety Act to create a new kind of information notice. It inserts new subsection (C1) creating a duty for OFCOM to issue an information notice to a provider of a service which falls within new subsection (E1) requiring the recipient to ensure retention of information relating to the use of the service by a child who has died.

879 New subsection (C1) also gives OFCOM the power to issue a notice to a "relevant person" as defined in s.101(7) of the Online Safety Act in order to ensure the retention of information relating to the use of a service within subsection (E1). This may include, for example, ex-providers of the service where relevant.

880 New subsection (A1) sets out the circumstances in which the duty or power to issue an information notice under new subsection (C1) applies. It also defines the term "investigating authority" as the senior coroner (in England and Wales), a procurator fiscal (in Scotland) or a coroner (in Northern Ireland).

881 New subsection (B1) sets out the details which the investigating authority needs to provide to OFCOM in order for subsection (C1) to apply, this includes information which will assist recipients of these information notices in identifying the relevant data and the details of any regulated service which has been brought to the investigating authority's attention as being of interest in connection with the child's death.

882 New subsection (D1) clarifies that the requirement to ensure the retention of information under a notice issued under subsection (C1), involves actively taking reasonable and timely steps to prevent the deletion of such information. This includes addressing both intentional deletion and potential deletion through routine systems or processes.

883 New subsection (E1) sets out the two ways in which a regulated service falls within scope of the new information notice provision; either it falls under a regulated service type defined by the Secretary of State in regulations, or it is a regulated service specifically notified to OFCOM by the investigating authority as per new subsection (B1)(d).

884 New subsection (F1) sets out the type of information that must be retained under the new information notice. The information must either fall within the kind of information which OFCOM can access under its existing powers under s.101(1) of the Online Safety Act 2023 or be the kind that a person might need to retain in order to respond to a notice under subsection (1) in future.

885 Subsection 3(b) of clause 122 makes a consequential amendment to s.101(3) of the Online Safety Act 2023 making it clear the new provisions inserted by subsection 3(a) include a power to obtain or generate information.

886 Subsection 3(c) inserts new subsection (5A) confirming that an information notice issued under s.100(C1) must not require processing of information which could contravene the data protection legislation (as defined in s.236(1) of the Online Safety Act.

887 Subsection (4) amends section 102(1) of the Online Safety Act 2023 bringing notices issued under subsection 101(C1) within the definition of an "information notice" for the purposes of the Online Safety Act 2023, subsection (10)(b) amends the definition in s.236(1) to reflect this

change. This means other provisions in the OSA relating to "information notices", including enforcement provisions, will also apply to notices issued under new subsection (C1).

888 Subsection (4)(b) amends section 102(3) of the Online Safety Act, to clarify that the requirements regarding information which must be included in information notices currently set out in section 102(3) only apply to information notices issued under sections 100(1) and 101(1) of the Online Safety Act. It also adds the requirement for OFCOM to specify when the information covered by such a notice must be provided. It then omits subsection 102(4) as that is now addressed in new 102(3)(ca).

889 Subsection (4)(d) inserts new subsections (5A), (5B) and (5C) into section 102. New subsection (5A) outlines specific requirements for information notices issued under new section 101(C1).

890 New subsection (5B) gives OFCOM the power to extend the duration for which a person is obligated to retain information if they have been issued an information notice under section 101(C1). The period can only be extended in response to information received from the investigating authority. The period can only be extended by a maximum of six months at a time.

891 New subsection (5C) explains how OFCOM can exercise the power granted in subsection (5B). They can do so by issuing a notice to the person who received the initial information notice under section 101(C1). This notice specifies the further period for information retention and provides the reason for the extension. Importantly, there is no limit on how many times OFCOM can use this power.

892 Subsection (4)(e) of clause 122 introduces a new subsection (9A) into section 102 which requires OFCOM to cancel an information notice under new subsection 101(C1) if the investigating authority advises OFCOM that the information specified in an information notice under section 101(C1) is no longer necessary to be retained. This cancellation is communicated through a notice to the person who initially received the information notice.

893 Subsection (4)(f) amends section 102(10) adding a definition of the term "the investigating authority," clarifying that it has the same meaning as defined in section 101.

894 Subsection (5) makes amendments to section 109 (offences in connection with information notices). These amendments introduce new subsections (6A) and (6B) to section 109.

895 Subsection (6A) establishes an offence: if a person, who has been issued an information notice under section 101(C1), deletes or alters information required to be retained, and their intention is to prevent the information's availability for an official investigation into the death of the child, they commit an offence. Subsection (6B) clarifies that information is considered deleted if it is irrecoverable, regardless of how it occurred.

896 Subsection (6) amends section 110 (senior managers' liability: information offences), introducing a new subsection (6A) to section 110. It establishes an offence for an individual named as a senior manager of an entity if the entity commits an offence under section 109(6A), and the individual fails to take all reasonable steps to prevent that offence. Section 109(7) is amended to reflect the inclusion of the new offence under new subsection (6A).

897 Subsection (7) amends s.113(2) (penalties for information offences) to include the new offences in s.109(6A) and s.110(6A).

898 Subsection (8) omits the definition of data protection legislation currently in s.114 of the Online Safety Act, and subsection (10)(a) moves that definition to s.236(1). Subsection (11)

then amends s.237 (index of defined terms) to include the definition of data protection legislation now in s.236.

899 Subsection (9) amends s.225 (Parliamentary procedure for regulations) to confirm that the regulations made by the Secretary of State under new s.101(E1) are subject to the negative procedure.

Information for research about online safety matters

Clause 123: Information for research about online safety matters

900 Clause 123 inserts new section 154A into the Online Safety Act 2023 to allow creation of a new framework that would permit researchers access to information held by certain providers of internet services, for the purposes of research into online safety matters.

New section 154A – information for research about online safety matters

901 Subsection (1) gives the Secretary of State the power to make regulations requiring providers of regulated services to provide information to independent researchers for them to carry out associated research. The information will be provided under a new framework created by the regulations.

902 Subsection (2) gives examples of the type of provision the regulations might make, including matters of procedure, fees, enforcement and appeals. This is a non-exhaustive list of examples to give an indication of the types of matters to be set out in the regulations.

903 Subsection (3) sets out a non-exhaustive list of the types of enforcement measures that the regulations might include, including potential financial or criminal liability.

904 Subsection (4) makes provision for the appointment of an appropriate person (defined in subsection 8(b) as OFCOM or such other person or body as the Secretary of State may consider appropriate) to carry out functions under, or for the purposes of, the regulations.

905 Subsection (5) confirms that the regulations may apply generally, or only to those descriptions of regulated services, researchers, research, or information as are specified in the regulations. It also sets out that the regulations may apply differently to each of these stated services, researchers, research, or information.

906 Subsection (6) makes it clear that the regulations made under this power shall not require providers to do anything that would contravene data protection legislation or result in the disclosure of legally privileged material.

907 Subsection (7) requires the Secretary of State to consult several named organisations and groups before making the regulations.

908 Subsection (8) defines the term 'independent research' as research carried out other than on behalf of a regulated service. It also defines 'appropriate person' for the purposes of new section 154A(4).

909 Subsection (3) of clause 123 removes OFCOM's duty to produce guidance under section 162(7) to (10) of the Online Safety Act 2023. Under section 162(1) to (6) of that Act, OFCOM must produce a report exploring what information is currently available to researchers, what factors are constraining their research, and what can be done in the future to improve access to data. The removal of OFCOM's requirement to produce guidance following publication of that report is intended to avoid any conflict between the guidance and any regulations made under new section 154A(1).

910 Subsection (4) makes provision in relation to parliamentary procedure. It requires the first set of regulations made to be subject to the affirmative parliamentary procedure. Any subsequent regulations, which are unlikely to amend significant policy detail of the regime, would then be made through the negative parliamentary procedure.

911 Subsection (5) states that the consultation required under new section 154A(7) can be conducted before the Digital (Use and Access) Bill is passed.

Retention of biometric data

Clause 124: Retention of biometric data and recordable offences

912 Clause 124 makes changes to Part 1 of the Counter-Terrorism Act (CTA) 2008. Section 18A(3) of the CTA sets out that where an individual has a conviction for a recordable offence their biometric data (fingerprints and DNA profiles) can be retained indefinitely (unless the conviction is exempt). This is consistent with similar provisions in the Police and Criminal Evidence Act 1984 which set out the retention framework for biometric data retained for broader criminal investigations in England and Wales (the relevant provisions of CTA 2008 apply only to biometric data that is retained for the purposes of national security). However, section 18A(3) does not apply to individuals who received their conviction overseas or in Scotland. Clause 124 makes changes to the sections 18A and 18E CTA 2008 to enable the indefinite retention of biometric data that relates to an individual who has an overseas conviction that is equivalent to a conviction for a recordable offence (section 18E(1) provides a definition of a recordable offence in either England and Wales or in Northern Ireland).

913 Subsection (2) amends section 18A(3) so that it applies to convictions for recordable-equivalent offences as well as for recordable offences.

914 Subsection (4) amends section 18E(1) to provide a definition of a recordable-equivalent offence. Recordable-equivalent offences are offences committed other than in England and Wales or Northern Ireland, if the act in question would constitute a recordable offence if it had been committed in England and Wales or Northern Ireland.

915 Subsections (5) to (9) make certain amendments to section 18E in connection with the amendment made by subsection (4).

916 Subsection (10) inserts new subsection (7A) into section 18E to recognise qualifying-equivalent offences. Section 18A(3) does not allow for the indefinite retention of biometric data of persons who have only one conviction, if they were under the age of 18 when they committed the offence in question. However, this exemption does not apply to "qualifying offences" (section 18E(7) defines this term). The purpose of the amendment made by subsection (10) is to ensure that overseas convictions for offences that correspond to qualifying offences are not exempt for the purposes of section 18A(3).

917 Subsections (11) – (13) make provision for retrospective application. Subsection (11) sets out that amendments made by this clause also apply retrospectively to biometrics received in the three years before commencement of the section. Subsections (12) and (13) set out that, where a law enforcement authority is holding section 18 material which it received in the three years before the commencement day, they can retain and use the biometric data. However, the effect of subsection (13)(b) is that the authority cannot use the biometric data in criminal proceedings instituted before the commencement day in England and Wales, Northern Ireland or Scotland, or in any criminal proceedings in any other country or territory at any point.

918 Clause 136 sets out that clause 124 will come into force on Royal Assent of the Bill.

Clause 125: Retention of pseudonymised biometric data

919 Clause 125 makes changes to Part 1 of the Counter-Terrorism Act (CTA) 2008. Section 18A(4) CTA 2008 provides that where a law enforcement authority is processing biometric data (fingerprints and DNA profiles) under the CTA 2008 and does not know the identity of the individual to whom the biometric data relates, and has never known the identity, they may retain the biometric data indefinitely (data that is held in such a form may be referred to as being held in a "pseudonymised form"). Pseudonymised biometric data can be used by the police to wash (i.e. checked) against other biometric data, for example against biometric material that is submitted against visa or asylum applications. Section 18A(5) sets out that where a law enforcement authority comes to know the identity of the individual to whom the biometrics relate, and where the individual has no previous convictions, the authority is permitted to retain the biometrics for three years (the standard retention period within the CTA 2008) from that time; following which they must either destroy the data or make a national security determination to retain it.

920 Subsection (5) of this clause inserts new subsections (7) to (9) into Section 18A. New subsection (7) sets out that biometric data may be retained indefinitely by the law enforcement authority in cases where such biometric data is acquired from an overseas law enforcement authority in a format which identifies the individual to whom the data relates, but the law enforcement authority takes the necessary steps to pseudonymise the biometric data as soon as reasonably practicable after receipt. These steps must remove any identifiable information relating to the biometric data. If the law enforcement authority is in a position to identify the individual in question using other information that it holds, the effect of new subsection (7)(d) is that the authority cannot rely upon this new retention provision.

921 Subsection (6) makes a consequential amendment to section 18E(1) to insert a new definition of an overseas law enforcement authority.

922 Subsections (7) to (12) make provision for the retrospective application of Clause 125, enabling a law enforcement authority to apply the section to existing biometric data and retain data if it pseudonymises it as soon as reasonably practicable after the commencement of the section. Subsection (8) limits retrospective application to biometric data obtained or acquired in the three years before commencement of the section.

923 Subsections (9) and (10) set out when a law enforcement authority is required to pseudonymise biometric data that it obtained prior to the commencement of this section to be able to apply the provisions of the section to that data.

924 Subsections (11) and (12) make provision in relation to the use of biometric data that was obtained in the three years before the commencement of the section, but that the law enforcement authority was, prior to commencement, required to destroy. For example, in a case where an overseas law enforcement authority supplies the authority with biometric data that was taken almost, or even more than, 3 years ago. The effect of subsection (12)(a) is that the authority may continue to retain and use the material (in so far as it is possible to use material that is not in an identifiable form). Subsection (12)(b)(i) provides that such legacy biometric data may not be used in criminal proceedings instituted before the commencement day in England and Wales, Northern Ireland, or Scotland. This includes criminal trials that are ongoing at the date of commencement, and retrials that take place after commencement (for example, where a prior conviction has been quashed). Subsection (12)(b)(ii) provides that

legacy biometric data may not be used in any criminal proceedings in any other country or territory, even if the proceedings were instituted after commencement of the section.

Clause 126: Retention of biometric data from INTERPOL

925 Clause 126 inserts a new section into the Counter-Terrorism Act (CTA) 2008 (new section 18AA) to vary the regime governing the retention of biometric material obtained through INTERPOL co-operation . New section 18AA sets out updated retention rules for biometric data that has been received through INTERPOL. The NCA, in its capacity as the UK's National Central Bureau, receives daily notifications from INTERPOL of all new, updated and cancelled notices and diffusions. INTERPOL notices are international requests for cooperation or alerts allowing police in member countries to share critical crime-related information, including information relating to national security cases, e.g. counter-terrorism investigations. Member countries may also request cooperation from each other through another alert mechanism known as a 'diffusion'. This is less formal than a notice and is circulated directly by a National Central Bureau to all or some member countries. INTERPOL notices or diffusions may include biometric materials, for example fingerprints.

926 Subsection (2) makes a consequential amendment to section 18A(4) CTA 2008, to recognise the new retention power provided by new section 18AA.

927 Subsection (3) inserts new sections 18AA and 18AB into the CTA 2008. New section 18AA(1) defines the biometric data to which the new section applies (subsection (1) refers to "section 18 material" - see section 18(2) CTA 2008 for a definition of that term). Subsection (1) is intended to apply to section 18 material that is provided as part of a notice or a diffusion.

928 New section 18AA(2) provides that a law enforcement authority may retain the biometric data received from INTERPOL until the UK National Central Bureau (NCB) informs the authority that the INTERPOL notice or diffusion has been cancelled or withdrawn. At this point, the law enforcement authority must either delete the biometric data from its systems, or it may make a National Security Determination, under section 18B CTA 2008 to authorise its retention for a period of time.

929 New section 18AA(3) makes equivalent provision for cases where the law enforcement authority is also the NCB.

930 New section 18AA(5) clarifies that new section 18AA(1) also applies to biometric data that is not provided with an initial notification or diffusion, but that is provided subsequently as part of that request etc.

931 Subsection (3) of clause 126 also inserts a new section 18AB into the CTA. Section 18AB confers a delegated power on the Secretary of State to make changes by secondary legislation to amend section 18AA where there are changes to INTERPOL's name or its processes in relation to the processing or sharing of INTERPOL biometrics with member countries. For example, if INTERPOL was to adopt alternative forms of co-operation to its current notices and diffusions, this power would enable any consequential amendments to section 18AA that are necessary. Such secondary legislation will be subject to the affirmative procedure.

932 Subsection (4) makes a consequential amendment to section 18BA(5) CTA 2008.

933 The effect of subsection (5) is that new section 18AA will apply to biometric data received via INTERPOL prior the commencement of this section, if the request or threat to which the data relates remains outstanding. Subsections (6) and (7) make provision to enable a law enforcement authority to continue to retain and use (in accordance with section 18D(1) CTA

2008) biometric data relating to live requests for co-operation etc. even if the requirement to destroy the material arose prior to the commencement of this section. However, such legacy material may not be used in evidence against the person to whom the material relates in criminal proceedings that were instituted before the commencement day or for any criminal proceedings in another country at any time.

934 Clause 136 sets out that Clause 126 will come into force on Royal Assent of the Bill.

Trust services

Clause 127: The eIDAS Regulation

935 The term "the eIDAS Regulation" in the clauses described 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, as retained by the EUWA 2018, and amended by The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 S.I. 2019/89.

936 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 128: Recognition of EU conformity assessment bodies

937 Clause 128 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 129: Removal of recognition of EU standards etc

938 Clause 129 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 130: Recognition of overseas trust products

939 Clause 130 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 certain 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.

940 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.

941 Clause 130 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.

942 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.

943 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.

944 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 131: Co-operation between supervisory authority and overseas authorities

945 Clause 131 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.

946 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 legislation.

Clause 132: Time periods: the eIDAS Regulation and the EITSET Regulation

947 Subsection (1) inserts Article 3A into eIDAS Regulation. New Article 3A provides that the rules of interpretation for periods of time in Article 3 of Regulation No 1182/71 (the 'Time Periods Regulation') apply to relevant time periods under eIDAS Regulation.

948 Subsection (3) amends regulation 2 of the Electronic Identification and Trust Services for Electronic Transactions Regulation 2016 (S.I. 2016/696) (the '2016 Regulations') to apply the

rules under Article 3 of the Time Period Regulations also to relevant periods under the 2016 Regulations.

949 Subsection (4) make some minor changes to Schedule 1 (monetary penalties) to the 2016 Regulations to ensure consistency and clarity in calculation of time periods.

Part 8: Final provisions

Clause 133: Power to make consequential amendments

950 Clause 133 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 134: Regulations

951 Clause 134 makes provision concerning the form and procedure for making regulations under the powers in the Bill.

Clause 135: Extent

952 Detailed analysis of the extent of the Bill can be found at Annex A. Otherwise, clause 135 is self-explanatory.

Clause 136: Commencement

953 Clause 136 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 137: Transitional, transitory and saving provision

954 Clause 137 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 9 to this Bill (Transfers of personal data to third countries etc: consequential and transitional provision).

Clause 138: Short title

955 Clause 138 is self-explanatory.

Schedules

Schedule 1: National Underground Asset Register (England and Wales): monetary penalties

956 This Schedule inserts a new Schedule 5A into the New Roads and Streets Act 1991 which makes provisions about the monetary penalties for non-compliance with the requirements to pay a fee and provide information set out in Part 3A of the Act. The penalty scheme is intended to be a simple and effective approach which can easily be applied in practice.

957 Paragraph 1(1) confers a power on the Secretary of State to issue a "penalty notice" where a person has failed to comply with a requirement to pay a fee in accordance with regulations under section 106D(1), or failed to provide information in accordance with regulations under section 106E(1) or (2). A notice can also be issued where such information is either misleading or false.

958 The Secretary of State will have discretion over whether to impose a penalty. There will also be a requirement for a "warning notice" to be given to the person concerned where the imposition of a penalty is being proposed, together with provision for a period during which written representations can be made. Thereafter the Secretary of State has six months within which a "penalty notice" can be given to the person. Among other things, a penalty notice must state the amount of the penalty.

959 Paragraph 1(2) in Schedule 5A empowers the Secretary of State to set out, in regulations, the amount of any penalty to be imposed. Should any person then be in breach of a relevant requirement, and the Secretary of State is considering the imposition of a monetary penalty, the amount of such a penalty will be that which is already provided for in existing regulations. The Secretary of State may not give more than one penalty notice to a person in respect of the same breach of the relevant requirement.

960 Paragraph 4 of Schedule 5A makes provision for the enforcement of the penalty notice. Paragraph 5 sets out a person's right of appeal against the penalty notice (or any requirement of it); such an appeal can be made to the First-tier Tribunal on any of the grounds set out in paragraph 5(2). Further provision is also made as to the Tribunal's powers in respect of such an appeal and the effect of the Tribunal's decision.

Schedule 2: National Underground Asset Register (Northern Ireland): monetary penalties

961 This Schedule inserts a new Schedule 2ZA into the Street Works (Northern Ireland) Order 1995 which makes provisions about the monetary penalties for non-compliance with the requirement to pay a fee in accordance with regulations under Article 45D(1), and the requirement to provide information in accordance with regulations under Article 45E(1) or (2). Schedule 2ZA therefore makes equivalent provision to the new Schedule 5A inserted into the 1991 Act by Schedule 1 (see paragraph (956) above).

Schedule 3: Registers of births and deaths: Minor and consequential amendments

962 Part 1 of Schedule 3 makes a number of amendments to the BDRA including: amending sections of the BDRA which referred to the registrar or superintendent registrar, or officer, having "custody of the register" and replacing such references with "relevant registration officer for the register", "the relevant registration officer" or "the appropriate registration officer". Other amendments specify how indexes need to be created and retained by both the Registrar General and the superintendent registrar.

963 Part 2 of Schedule 3 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 4: Lawfulness of processing: Recognised legitimate interests

964 Schedule 4 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 70). The amendment made to Article 6(1) by clause 70(2)(ac) ensures that public authorities cannot rely on these conditions when processing in the performance of their tasks.

965 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.

966 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.

967 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.

968 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.

969 Paragraph 6 provides a condition for processing where it 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 1.

970 Paragraphs 7 and 8 elaborate on what these concepts mean.

Schedule 5: Purpose Limitation: Processing to be treated as compatible with original purpose

971 Schedule 5 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)).

972 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.

973 Paragraph 2 treats further processing as compatible when it is necessary for the purpose of making a disclosure of personal data for the purpose of archiving in the public interest. Some

organisations may have originally collected personal data under the consent lawful ground for their own purposes, e.g. commercial purposes, without at the time realising its future historical value to an archive. This provision will enable such organisations to disclose the data to controller ("R"), provided that "R" makes the request that states they intend to only process the personal data for the purpose of archiving in the public interest; that the disclosure is carried out in accordance with the provisions in Article 84B; and that the personal data in question was collected by the disclosing controller under the consent lawful ground. The controller making the disclosure must also reasonably believe that "R" will process the data in accordance with generally recognised standards that are relevant to R's work of archiving in the public interest.

974 Paragraph 3 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.

975 Paragraphs 4 and 5 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.

976 Paragraph 6 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.

977 Paragraph 7 treats further processing as compatible where it is necessary for the purposes of protecting the vital interests of the data subject or another individual.

978 Paragraph 8 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 10.

979 Paragraph 11 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.

980 Paragraph 12 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 6: Automated decision-making: minor and consequential amendments

981 Schedule 6 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 in the new Article 22A-D UK GDPR and sections 50A-D DPA 2018, in clause 80.

982 Paragraph 2(6) and paragraph 13(4) of schedule 6 extends the provision at Article 12 (6) UK GDPR and section 52(4) DPA 2018 to enable the controller to request additional information to confirm the identity of the data subject to requests made under the new Article 22A-D and 50C or 50D.

Schedule 7: Transfers of personal data to third countries etc: General processing

983 Chapter 5 of the UK GDPR sets out the conditions under which personal data can be lawfully transferred to a country outside of the UK or an international organisation (as defined in Article 4 of UK GDPR). Schedule 7 makes various amendments to Chapter 5 of the UK GDPR, to reform the UK's regime for international transfers, as explained below.

984 Paragraph 2(1) of Schedule 7 omits Article 44 and paragraph 2(2) replaces it with a new Article 44A.

985 Article 44A(1) to (3) 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 that 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.

986 Paragraph 3 of Schedule 7 omits Article 45. Article 45 currently provides that transfers of personal data to another country can take place where the Secretary of State has made regulations finding that the country in question provides an adequate level of protection for personal data. The free flow of personal data is then allowed to this country.

987 In place of Article 45 and sections 17A and 17B of the DPA 2018, which are omitted by paragraphs 12 and 13 of Schedule 9, paragraphs 4 and 5 of Schedule 7 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 7 and Schedule 9 will be that all provisions relating to the approval of transfers to other countries or international organisations will be contained in Chapter 5 of the UK GDPR.

Approving transfers of personal data

988 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.

989 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.

990 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 the Secretary of State must be satisfied that the standard of protection in the other country, viewed as a whole, is not materially lower than the standard of protection in the UK, the wider context of data flows between the UK and another country may be important when deciding whether to make regulations.

991 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.

992 Article 45A(5) provides that regulations under Article 45A are subject to the negative resolution procedure.

The data protection test

993 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.

994 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 replication 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.

995 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.

996 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.

997 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).

998 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

999 Paragraph 5 of Schedule 7 inserts Article 45C into the UK GDPR, replacing section 17B of the DPA 2018 which has been omitted by paragraph 13 of Schedule 9.

1000 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.

1001 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.

1002 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.

1003 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

1004 Paragraphs 6 to 8 of Schedule 7 amend Article 46 and 47 of the UK GDPR and introduces new Article 47A.

1005 Paragraph 6(1) is self-explanatory.

1006 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.

1007 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 (i.e. the transfer mechanisms described in Articles 46(2) or (3), such as standard data protection clauses specified in a document issued by the ICO, or specified in regulations pursuant to new Article 47A(4)) are provided in connection with the transfer. If the safeguards are provided by a legally binding and enforceable instrument between a UK public body and another person or persons (under Article 46(2)(a)), the transfer must be consistent with the intended scope of that instrument; and 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 transfers which is intended to be made in reliance on the instrument.

- Where the safeguard is a mechanism described in 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.

1008 Paragraphs 6(4)(a)(i), (e) and (f) of Schedule 7 make consequential amendments to Article 46(2) to clarify that the word 'safeguards' refers only to the transfer mechanisms listed in 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.

1009 Paragraph 6(5)(a) makes a consequential amendment to Article 46(3) to clarify that the word 'safeguards' refers only to the transfer mechanisms listed in 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.

1010 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. 1060 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 public bodies that are parties to an instrument under 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.

1011 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.

1012 Paragraph 7 is self-explanatory.

Making provision about further safeguards for transfer

1013 Paragraph 8 of Schedule 7 inserts Article 47A, which makes further provision about transfers subject to appropriate safeguards.

1014 New Articles 47A(1) to (3) restate existing sections 17C(1), (2) and (3) of the DPA 2018, which are omitted by Schedule 9. 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 7 and Schedule 9 will be that all provisions relating to transfers subject to appropriate safeguards will now be contained in Chapter 5 of the UK GDPR.

1015 New Article 47A(4) to (7) provides a power for the Secretary of State to make provision, by way of regulations (subject to the 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

1016 Paragraph 9 of Schedule 7 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.

1017 Paragraph 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

1018 Paragraph 10 of Schedule 7 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 8: Transfers of personal data to third countries etc: Law enforcement processing

1019 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 8 makes various amendments to Chapter 5, to reform the UK's regime for international transfers for law enforcement purposes, as explained below.

1020 Paragraph 2 of Schedule 8 amends section 72(1)(b) of the DPA 2018, by substituting "special conditions that apply" with "additional conditions that apply in certain cases" and by referencing section 73(4)(b). These changes are relevant to amendments made to section 73(4)(b) and section 77.

1021 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 section are met. The general conditions for transfer remain broadly the same, with minor and technical amendments made to provide greater clarity. 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, or essential interests of a third country or the UK, and where the authorisation cannot be obtained in good time. In such circumstances, the controller must notify the overseas authoriser as soon as reasonably practicable.

1022 Paragraph 3 also amends condition 3 in s.73(4) by expanding the list of intended recipients to specifically include processors acting on behalf of, and in accordance with a contract with, a controller. Whilst transfers to processors in third countries are currently permissible, this amendment clarifies the existing law and provides legal certainty to UK controllers that they can transfer personal data to their processors operating outside of the UK.

1023 Paragraph 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 7 above, so reference should be made to those notes if a more detailed explanation on the effect of these provisions is required.

1024 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 data protection safeguards to make a transfer of personal data to that country or international organisation, provided the transfer falls within the terms of the regulations.

1025 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.

1026 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.

1027 Paragraph 5 of Schedule 8 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.

1028 Paragraph 6 of Schedule 8 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. Paragraph 6 introduces new subsections to this provision.

1029 Paragraphs 6(1) and 6(2) are self-explanatory.

1030 Paragraph 6(3) 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) 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:

- 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);
- or (b)) 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);

1031 Paragraphs 6(5) and 6(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 still be required to inform the Commissioner of the categories of data to be transferred where the

controller determination mechanism is relied upon), except where the transfer is to a processor pursuant to the new section 73(4)(aa). 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(1A)(b).

1032 Paragraph 6(7) adds new sections 75(4), 75(5), 75(6) and 76(7).

1033 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)(a). 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.

1034 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 reached 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 replication of protections for data subjects, which would not be reasonable or proportionate given the ways in which data protection regimes may differ.

1035 Paragraph 6(7) 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)(b), 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.

1036 Paragraph 6(7) introduces new section 75(7), which clarifies that references to the protection for the data subject are to that protection taken as a whole.

1037 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.

1038 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.

1039 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.

1040 Paragraph 8 amends the italic heading before section 77 from "Transfers to particular recipients" to "Additional conditions".

1041 Paragraph 9 amends the heading of section 77 from "Transfers of personal data to persons other than relevant authorities" to "Additional conditions for transfers in reliance on section 73(4)(b)". Paragraphs 9(1) and (2) amend sections 77(6) and (7) to specify that they relate to transfers that take place in reliance on section 73(4)(b).

1042 Paragraph 10 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.

1043 Paragraph 10(2) inserts new subsection 78(A1) which clarifies that subsections (1) to (6) apply where transfers are conducted under section 73, except where the transfer is to a processor pursuant to section 73(4)(aa).

1044 Paragraph 10(3) amends section 78(1) to allow subsequent transfers to be made without authorisation in the exceptional circumstances set out in section 78(1A). Where such transfers are made, the UK authoriser must be informed without delay.

1045 Paragraph 10(4) inserts new section 78(1A) stipulating 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.

1046 Paragraph 10 (7) makes a minor amendment to the wording in section 78(4) but maintains the principle that the UK authoriser may not give permission for a subsequent transfer without the prior authorisation of the EU member State where the data originated. 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, or essential interests of a third country or the UK, and where the authorisation cannot be obtained in good time. In such circumstances, the controller must notify the overseas authoriser as soon as reasonably practicable.

1047 Paragraph10(8) amends section 78(5)(a) whereby 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.

1048 Paragraph 10(10) inserts a new section 78(7) which specifies the conditions that controllers must impose when making transfers to processors pursuant to s. 73(4)(aa).

Schedule 9: Transfers of personal data to third countries etc: minor and consequential amendments and transitional provision

1049 Part 1 of Schedule 9 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 7 and Schedule 8 (as explained earlier in these Explanatory Notes).

1050 Part 2 of Schedule 9 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.

1051 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.

1052 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.

1053 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.

1054 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).

1055 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 10: Complaints: minor and consequential amendments

1056 Schedule 10 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 section 164A and in clause 102.

Schedule 11: Further minor provision about data protection

1057 Schedule 11 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. It also amends the territorial extent of some provisions in the Victims and Prisoners Act 2024.

Schedule 12: Storing information in the terminal equipment of a subscriber or user

1058 Schedule 12 inserts new Schedule A1 to the Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PEC Regulations'). This schedule sets out exceptions to the prohibition on the storage of information, or access to information, on a user's terminal equipment in new regulation 6(1) of the PEC Regulations.

1059 Paragraph 1 of Schedule A1 sets out the meaning of "website" used in this schedule. It also cross-refers to regulation 6(2) which sets out interpretive provisions relevant to this schedule.

1060 Paragraph 2 of Schedule A1 reproduces the current consent exception in regulation 6(2) of the PEC Regulations. Organisations can store information or gain access to information stored in the terminal equipment of an individual, if the individual has been provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and the individual has given consent.

1061 Paragraph 3 of Schedule A1 reproduces the current transmission of a communication exception in regulation 6(4)(a) of the PEC Regulations.

1062 Paragraph 4(1) of Schedule A1 reproduces the current strictly necessary exception in regulation 6(4)(b) of the PEC Regulations. Sub-paragraph (2) provides a non-exhaustive list of examples of "strictly necessary" purposes for the purpose of this exception.

1063 Paragraph 5 of Schedule A1 introduces a new exception 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 (1)(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.

1064 Paragraph 6 of Schedule A1 introduces a new exception 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. Or, 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. This exception only applies 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.

1065 Paragraph 7 of Schedule A1 introduces a new exception 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.

Schedule 13: Privacy and electronic communications: Commissioner's enforcement powers

1066 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 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.

1067 Clause 113 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 by Schedule 13, which makes modifications to the enforcement provisions in the DPA 2018 for the purposes of their application to the PEC Regulations.

1068 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 a 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.

1069 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.

1070 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.

1071 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.

1072 Paragraph 5 of Schedule 1 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.

1073 Paragraphs 6 and 8 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.

1074 Clause 97 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.

1075 Clause 99 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.

1076 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.

1077 Paragraph 14 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.

1078 Paragraph 15 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) of the PEC Regulations, which are instead subject to a fixed monetary penalty.

1079 New subsection (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.

1080 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.

1081 Paragraph 17 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.

1082 Paragraph 18 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.

1083 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.

1084 Paragraph 19 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.

1085 Paragraph 20 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.

1086 Paragraph 21 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.

1087 Paragraph 22 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.

1088 Paragraph 23 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.

1089 Paragraph 24 makes modification to section 181 (Interpretation of Part 6) of the DPA 2018 for the purposes of its application to the PEC Regulations.

1090 Paragraph 25 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.

1091 Paragraph 26 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.

1092 Paragraph 27 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 27 are self-explanatory.

1093 Paragraph 28 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 28 are self-explanatory.

1094 Paragraph 29 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.

1095 Paragraph 30 sets out the meaning of "the PEC Regulations" for the purposes of Schedule 13.

Schedule 14: The Information Commission

1096 Paragraph 1 of Schedule 14 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).

1097 Paragraph 2 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.

1098 Paragraph 3 contains transitional provisions relating to the requirement under paragraph 3(4) of Schedule 12A to the DPA 2018 for the Secretary of State to consult the chair of the Information Commission prior to appointing non-executive members of the Commission. The transitional provisions allow the requirements under paragraphs 3(4) of

Schedule 12A to be satisfied by consultation carried out, before this Schedule comes into force, with the person who holds the office of Information Commissioner.

1099 Paragraph 4 contains transitional provisions relating to the consultation requirements under paragraph 25 of Schedule 12A to the DPA 2018 for the chair of the Information Commission to consult the Secretary of State before appointing the first chief executive of the Information Commission. The transitional provisions allow the requirements under paragraph 25 of Schedule 12A to be satisfied by consultation carried out, before Schedule 14 comes into force, by the person who holds the office of Information Commissioner.

New Schedule 12A to the Data Protection Act 2018: The Information Commission

1100 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.

1101 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.

1102 Paragraph 3 makes provision for the membership of the Commission.

1103 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.

1104 Paragraph 5 requires that the chair and other members of the Commission are selected on merit on the basis of fair and open competition.

1105 Paragraph 6 makes provision for conflicts of interest.

1106 Paragraph 7 makes provision for the tenure of the chair.

1107 Paragraph 8 makes provision for the tenure of the deputy chair.

1108 Paragraph 9 makes provision for the tenure of the other non-executive members.

1109 Paragraph 10 makes provision for the remuneration and pensions of the non-executive members.

1110 Paragraph 11 makes provision in relation to the terms and conditions of the executive members.

1111 Paragraph 12 makes provision for the appointment and in relation to the terms and conditions of other staff of the Information Commission.

1112 Paragraph 13 makes provision in relation to committees of the Commission.

1113 Paragraph 14 makes provision in relation to the delegation of functions of the Commission.

1114 Paragraph 15 makes provision regarding advice from committees.

1115 Paragraph 16 makes provision in relation to proceedings of the Commission and its committees.

1116 Paragraph 17 requires that the Commission makes arrangements for the keeping of records of proceedings.

1117 Paragraph 18 makes provision for disqualification for acting in relation to certain matters.

1118 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.

1119 Paragraph 20 provides that the Secretary of State may make payments to the Commission.

1120 Paragraph 21 makes provision regarding fees, charges, penalties and other sums received by the Commission in carrying out its functions.

1121 Paragraph 22 makes provision concerning the keeping of accounts.

1122 Paragraph 23 makes provision about the authentication of the Information Commission's seal and the presumption of the authenticity of documents.

1123 Paragraph 24 clarifies that the Information Commission may do things to facilitate the exercise of its functions.

1124 Paragraph 25 makes transitional provision for the appointment of an interim chief executive.

1125 Paragraph 26 relates to the interpretation of references to pensions, allowances and gratuities

Schedule 15: Information standards for health and adult social care in England

1126 Schedule 15 amends section 250 (powers to publish information standards) of the Health and Social Care Act 2012 (HSCA 2012).

1127 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.

1128 Paragraph 2(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.

1129 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).

1130 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.

1131 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.

1132 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.

1133 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.

1134 Paragraph 4 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.

1135 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 in keeping information confidential yet accessible where appropriate, and assuring its integrity).

1136 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.

1137 Paragraph 5 of Schedule 15 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.

1138 Paragraph 6 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.

1139 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.

1140 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.

1141 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.

1142 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.

1143 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).

1144 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.

1145 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.

1146 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.

1147 Subsection (2) enables the Secretary of State to make arrangements for a person prescribed by regulations to exercise some or all of those functions.

1148 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.

1149 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.

1150 Subsection (2) enables the regulations to provide for the scheme to be established and operated by a person ("operator") specified in the regulations.

1151 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.

1152 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 16: Grant of smart meter communication licences

1153 The proposed new powers for the GEMA (referred to here as "the Authority") are introduced into the Energy Act 2008, to ensure that the new provisions sit alongside the Secretary of State's existing powers in that Act to modify licence conditions for smart metering related matters.

1154 Schedule 16, Part 1 amends section 88 of the Energy Act 2008 to differentiate between the existing powers of the Secretary of State and the new powers of the Authority.

1155 Section 91A makes provision for the Authority to make regulations regarding the procedure to be followed in granting a successor smart meter communication licence via a competitive or non-competitive process. The approval of the Secretary of State is needed for the Authority to make such regulations. The negative parliamentary procedure will apply to any such regulations by virtue of section 105(1) of the Energy Act 2008.

1156 Section 91B makes further provision regarding any regulations made by the Authority to appoint a successor smart meter communication licence.

1157 Section 91C introduces a power for the Authority to make modifications to conditions of gas and electricity licences or documents maintained under those licences for the purposes of, or in preparation for the grant of a smart meter communication licence.

1158 Section 91D requires the Authority to consult on any proposed changes to conditions of gas and electricity licences or documents maintained under them prior to making the changes.

1159 Schedule 16, Part 2 amends the Gas Act 1986 and the Electricity Act 1989 and has the effect of removing the existing powers for the Secretary of State to make regulations regarding the process to be followed for the competitive award of a smart meter communication licence.

Commencement

1160 The majority of provisions in this Bill will be brought into force by regulations made by the Secretary of State.

1161 The following provisions will come into force on Royal Assent.

- Clause 78 (searches in response to data subjects' requests);
- Part 1 of Schedule 16 and section 120 (Grant of smart meter communication licences) so far as it relates to that Part;
- Clauses 124 to 126 (retention of biometric data);
- Part 8;
- any provisions that are needed to make regulations.

1162 The following provisions will come into force two months after Royal Assent:

- Clause 69 (consent to law enforcement processing);
- Clause 81 (logging of law enforcement processing);
- Clause 95 (notices from the Information Commissioner);
- Clause 96 (power of the Information Commissioner to require documents);

1163 Part 2 of Schedule 16 and section 120 so far as it relates to that part, will commence on the day on which the first regulations under section 91A(1) of the Energy Act 2008 (inserted by Part 1 of Schedule 1) come into force.

Financial implications of the Bill

1164 The Government estimates the Net Present Social Value (NPV) of all of the reforms to be approximately £10.0 billion across the 10 years, in 2024 prices with a 2024 base year.

1165 The Net Present Value to the Private Sector of all of the reforms in the bill is expected to be approximately £4.4 billion over the course of the 10 years after implementation in 2024 and in 2024 prices, with a 2024 base year. The majority of these cost savings come from the National Underground Asset Register, Digital Verification Services and Data Protection measures which are expected to decrease compliance costs and increase productivity levels within the economy.

1166 Analytical notes providing the rationale, purpose and expected impact of all interventions made are included in the Impact Assessment and will be available in the supporting documents to the bill. The Impact Assessment will be provided at Royal Assent, as per RPC guidance.

Access to customer data and business data

1167 The provisions on Smart Data in Part 1 includes provisions for regulations to impose fees on data holders and others (Clause 11) and to impose a levy on data holders and others (clause 12). These are intended to cover the costs incurred by decision-makers and enforcers in exercising their functions.

1168 These provisions aim to ensure schemes are self-funding and not reliant on public funds. Therefore, no financial impacts are otherwise calculated.

1169 The objective of the Government's policy is to enable new, and accelerate existing, Smart Data schemes, and create a common framework to increase legislative consistency for schemes. This is intended to improve poor consumer and business outcomes, increase competition, create greater opportunities for innovation, produce time saving for users, reduce costs, increase the quality of services, improve the security of data sharing and increase the trust in data sharing mechanisms.

Digital Verification Services

1170 The government estimates the NPV of the Digital Identity reforms to be approximately £4.3bn over 10 years, in 2024 prices with a 2024 base year.

1171 The objective of this policy is to allow people to prove things about themselves as quickly and securely as possible. By enabling this, the aim is to have a better functioning digital identity system, protect against fraud, enhance privacy and data minimization and promote inclusive solutions.

1172 The Government expects some public sector organisations to have direct familiarisation costs as a result of this legislation. The Government expects Departments to face indirect costs to open their databases for private sector checks if they wish to as a result of this legislation. There are also costs associated with the setting up and running the digital identity governance function until it becomes self-sustainable.

1173 The Government also expects some UK businesses to face indirect costs. For businesses that choose to become certified against the UK digital identities and attributes trust framework and registered in the Digital Verification Services register, there are one-off organisational change costs to familiarise with their legislation and adapt to the digital

verification system. The Government also expects UK businesses to face indirect annual costs in the form of fees levied by public sector organisations to connect to government-held datasets and to check data. These fees are intended to offset public sector costs and maintain value for money for the taxpayer.

National Underground Asset Register

1174 In the Impact Assessment, the government estimates that the NUAR service will deliver in excess of £4.6 billion (2024 prices) over the 10-year appraisal period of economic benefits. This will come through reduced cost of sharing data, reduced number of utility strikes and an increase in on-site efficiency. Through implementing NUAR legislation, the benefits are the efficiencies and cost savings from moving to a more streamlined and uniform digital process for accessing and sharing underground asset records from the current fragmented information sharing process. These will benefit asset owners and data consumers across both the public and private sector.

Registers of births and deaths

1175 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 £0.6m. The reforms of the birth and death registration system are expected to lead to total net savings of approximately £25.1m (PV) over 10 years in 2024 prices to the public sector.

Data protection

1176 The data protection measures are estimated to create productivity and compliance benefits through increased data use and reduced compliance burdens on businesses. Several of the data protection measures are expected to generate familiarisation costs as businesses digest and implement the regulatory changes. The government estimates the NPV of the Data protection reforms to be approximately £0.6bn over 10 years, in 2024 prices with a 2024 base year.

Information Commission

1177 The government estimates the NPV of the Information Commission reforms to be approximately -£14 million over 10 years, in 2024 prices with a 2024 base year.

1178 A portion of the reforms to the regulator, such as the changes to enforcement powers, data protection complaints and reviewing adequacy decisions, are expected to create some cost savings. However, net costs are expected to increase as they familiarise and adapt to the new legislation. All these costs form part of current budget arrangements.

Health and Adult Social Care System

1179 The government estimates the NPV of the heath care reforms to be approximately £138 million over 10 years, in 2024 prices with a 2024 base year. The benefits are to both the public sector from improved compliance with information standards in the health and social care sector, across all providers of care in England, including the NHS. These reforms aim to ensure that clinical information flows as safely, securely, and seamlessly as it does in leading digital platforms. The intended benefits to the individual will be from the enhancing the quality of care and safety for patients, as well as enable better informed clinical and care decision-making.

1180 The total cost of the regulation is estimated to be £202.9 million (present value), of which £61.2 million (present value) is cost to business (IT suppliers and private health and social care providers). The remaining £141.6 million (present value) is a cost to the public sector (NHS and public social care providers).

Researchers access to data

1181 It is estimated that the set-up costs for the policy will be approximately £0.5m as a result of familiarisation costs and adapting processes to make data available. These costs are incurred by the private sector only.

Enforcement provisions

1182 The Government estimates the impact to the public sector via enhancing the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security reforms to be approximately £0.4bn over 10 years, in 2024 prices with a 2024 base year.

Parliamentary approval for financial costs or for charges imposed

1183 This section will be completed when the Bill transfers to the House of Commons.

Compatibility with the European Convention on Human Rights

1184 Baroness Jones of Whitchurch, Parliamentary Under-Secretary of State for the Future Digital Economy and Online Safety, has made a statement pursuant to section 19 of the Human Rights Act 1998 that, in her view, the provisions of the Data (Use and Access) Bill are compatible with the rights under the European Convention on Human Rights.

1185 Issues arising as to the compatibility of the Bill with the Convention rights are dealt with in a separate memorandum. This has been published separately on Gov.uk on 24 October 2024.

Duty under Section 13C of the European Union (Withdrawal) Act 2018

1186 Baroness Jones of Whitchurch, Parliamentary Under-Secretary of State for the Future Digital Economy and Online Safety, is of the view that the Bill as introduced into the House of Lords does not contain provision which, if enacted, would affect trade between Northern Ireland and the rest of the United Kingdom. Accordingly, no statement under section 13C of the European Union (Withdrawal) Act 2018 has been made.

Duty under Section 20 of the Environment Act 2021

1187 Baroness Jones of Whitchurch, Parliamentary Under-Secretary of State for the Future Digital Economy and Online Safety, is of the view that the Bill as introduced into the House of Lords does not contain provision which, if enacted, would be environmental law for the purposes of section 20 of the Environment Act 2021.

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 Motion 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: ACCESS TO CUSTOMER DATA AND BUSINESS DATA							
Introductory							
Clause 1	Yes	Yes	In part	Yes	In part	Yes	Yes
Data regulations							
Clause 2	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 3	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 4	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 5	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 6	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 7	Yes	Yes	In part	Yes	In part	Yes	Yes
Enforcement							
Clause 8	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 9	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 10	Yes	Yes	In part	Yes	In part	Yes	Yes
Fees etc and financial assistance							
Clause 11	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 12	Yes	Yes	N/A	Yes	N/A	Yes	Yes
Clause 13	Yes	Yes	In part	Yes	In part	Yes	Yes
Financial services sector							
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
Supplementary							
Clause 18	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 19	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 20	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 21	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 22	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 23	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 24	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 25	Yes	Yes	In part	Yes	In part	Yes	Yes
Clause 26	Yes	Yes	In part	Yes	In part	Yes	Yes
Part 2: DIGITAL VERIFICATION SERVICES							
Introductory							
Clause 27	Yes	Yes	N/A	Yes	N/A	Yes	N/A
DVS trust framework and supplementary codes							
Clause 28	Yes	Yes	N/A	Yes	N/A	Yes	N/A
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
DVS register							
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
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
Information gateway							
Clause 45	Yes	Yes	Yes	Yes	N/A	Yes	N/A
Clause 46	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 47	Yes	Yes	Yes	Yes	N/A	Yes	N/A
Clause 48	Yes	Yes	N/A	Yes	Yes	Yes	N/A
Clause 49	Yes	Yes	In part	Yes	N/A	Yes	N/A
Trust mark							
Clause 50	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Supplementary							
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
PART 3: NATIONAL UNDERGROUND ASSET REGISTER							
Clause 56	Yes	Yes	Yes	No	N/A	No	N/A
Clause 57	Yes	Yes	Yes	No	N/A	No	N/A
Clause 58	No	No	N/A	No	N/A	Yes	Yes
Clause 59	No	No	N/A	No	N/A	Yes	Yes
Clause 60	Yes	Yes	Yes	No	N/A	Yes	Yes
PART 4: REGISTERS OF BIRTHS AND DEATHS							
Clause 61	Yes	Yes	N/A	No	N/A	No	N/A

Clause 62	Yes	Yes	N/A	No	N/A	No	N/A
Clause 63	Yes	Yes	N/A	No	N/A	No	N/A
Clause 64	Yes	Yes	N/A	No	N/A	No	N/A
Clause 65	Yes	Yes	N/A	Yes	N/A	Yes	N/A
PART 5: DATA PROTECTION AND PRIVACY							
Chapter 1: Data Protection							
Terms used in this Chapter							
Clause 66	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Definitions in the UK GDPR and the 2018 Act							
Clause 67	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 68	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 69	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Data protection principles							
Clause 70	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 71	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 72	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Processing of special categories of personal data							
Clause 73	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 74	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Data subject's rights							
Clause 75	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 76	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 77	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 78	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 79	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Automated decision-making							
Clause 80	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Logging of law enforcement processing							

Clause 81	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Codes of conduct							
Clause 82	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 83	Yes	Yes	N/A	Yes	N/A	Yes	N/A
International transfers of personal data							
Clause 84	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Safeguards for processing for research etc purposes							
Clause 85	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 86	Yes	Yes	N/A	Yes	N/A	Yes	N/A
National security							
Clause 87	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Intelligence services							
Clause 88	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 89	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Information Commissioner's role							
Clause 90	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 91	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 92	Yes	Yes	N/A	Yes	N/A	Yes	N/A
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
Enforcement							
Clause 96	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 97	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 98	Yes	No	N/A	No	N/A	No	N/A
Clause 99	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 100	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 101	Yes	Yes	N/A	Yes	N/A	Yes	N/A

Clause 102	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 103	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 104	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Protection of prohibitions, restrictions and data subject's rights							
Clause 105	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Miscellaneous							
Clause 106	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 107	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Chapter 2: Privacy and Electronic Communications							
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
Clause 111	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 112	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 113	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 114	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Part 6: THE INFORMATION COMMISSION							
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
Clause 118	Yes	Yes	N/A	Yes	N/A	Yes	N/A
PART 7: OTHER PROVISION ABOUT USE OF, OR ACCESS TO, DATA							
Information standards for health and social care							
Clause 119	Yes	No	N/A	No	N/A	No	N/A
Smart meter communication services							
Clause 120	Yes	Yes	No	Yes	No	No	N/A
Information to improve public service delivery							
Clause 121	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Retention of information by providers of internet services							
Clause 122	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Information for research about online safety matters							
Clause 123	Yes	Yes	No	Yes	No	Yes	No
Retention of biometric data							
Clause 124	Yes	Yes	N/A	Yes (extends but does not apply to Scotland)	N/A	Yes	N/A
Clause 125	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 126	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Trust services							
Clause 127	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 128	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 129	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 130	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 131	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 132	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Part 8: FINAL PROVISIONS							
Clause 133	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 134	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 135	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 136	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 137	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 138	Yes	Yes	N/A	Yes	N/A	Yes	N/A
SCHEDULES							
Schedule 1	Yes	Yes	Yes	No	N/A	No	N/A
Schedule 2	No	No	N/A	No	N/A	Yes	Yes
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	Yes	N/A	Yes	N/A
Schedule 11	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Schedule 12	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Schedule 13	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Schedule 14	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Schedule 15	Yes	No	N/A	No	N/A	No	N/A
Schedule 16	Yes	Yes	N/A	Yes	N/A	No	N/A

Subject matter and legislative competence of devolved legislatures

Access to customer data and business data

1188 Part 1 of the Bill, so far as it relates to the supply or provision of goods, services and digital content to a consumer, falls within the consumer protection reservation in Section C7 of Schedule 5 to the Scotland Act 1998 and Section C6 of Schedule 7A to the Government of Wales Act 2006 as relating to the regulation of the sale and supply of goods and services to consumers. These reservations do not apply in relation to the potential regulation under Part 1 of the supply or provision of goods, services or digital to business customers.

1189 The power in clause 12 (levy) to impose, or provide for a specified public authority to impose, a levy is a tax-raising power and is therefore reserved as respects Scotland and Wales under the fiscal, economic and monetary policy reservations in Sections A1 of Schedules 5 and 7A to those Acts.

1190 The financial services sector clauses 14 to 17 relate to financial services and are therefore reserved as respects Scotland and Wales under the financial services reservations in Sections A3 of those Schedules. Those clauses are also fall under the financial services reservation in paragraph 23 of Schedule 3 to the Northern Ireland Act 1998.

1191 The subject matter of Part 1 is otherwise devolved and, to that extent, is subject matter in relation to which the Government will seek a Legislative Consent Motion (LCM) from the Scottish Parliament, the Senedd Cymru and the Northern Ireland Assembly.

Digital Verification Services

1192 The internet services reservation in relation to Scotland, Wales and Northern Ireland applies to digital verification services.

1193 These clauses regulate the provision of digital verification services, where providers of those services wish to appear on a government register, through the creation of a trust framework, supplementary codes, 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. The reservation of internet services applies in Northern Ireland, Wales and Scotland.

1194 Whilst the majority of the clauses fall within the internet services reservation, clause 47 and clause 48 are provisions which have been included to protect the confidential nature of information held by the Welsh Revenue Authority and Revenue Scotland, a devolved purpose. As such, these fall within the legislative competence of the Welsh and Scottish Parliaments respectively, and an LCM will be required. It is agreed that clauses 45 and 49(3) modify the executive competence of Devolved Welsh Authorities, and so under the Devolution Guidance Note for Wales an LCM is required.

National Underground Asset Register

1195 Legislative competence for the subject matter of Part 3 of the New Roads and Street Works Act 1991 (transport and street works) is devolved to Wales. As these provisions make amendments to the 1991 Act (including Part 3) in relation to this devolved subject matter, the LCM process will be engaged in relation to Wales. The relevant legislation for Northen Ireland is the Street Works (Northern Ireland) Order 1995 ("the 1995 Order"). Similarly, as these

measures make amendments to this Order, dealing with the transferred matter of transport and street works, the LCM process will be engaged in relation to Northern Ireland.

1196 The effective implementation and operation of NUAR will require the Secretary of State to exercise a range of functions, including a number of regulation-making powers. These will comprise a combination of existing powers, already found in the relevant legislation, and new powers inserted by this Bill. Some of these existing powers in the relevant legislation are, at present, solely conferred on the Welsh Ministers or the Northern Ireland Executive (in relation to Wales or Northern Ireland, as the case may be).

1197 The NUAR clauses in the Bill will make some of these existing powers, which are solely exercisable by the Welsh Ministers or the Department for Infrastructure in Northern Ireland (as the case may be), concurrently exercisable with the Secretary of State; this is to reflect that these existing powers will be used by the Secretary of State to implement NUAR, but could also be used for other purposes by the relevant devolved administration ("mixed purposes powers"). The clauses will also confer some new mixed purposes powers on the Secretary of State; provision is also made for these new mixed purpose powers to be concurrently exercisable by the Welsh Ministers and Department for Infrastructure for Northern Ireland. The NUAR clauses also remove existing (but uncommenced) powers from the Welsh Ministers and the Department for Infrastructure in Northern Ireland. This is in parallel with such powers also being removed from the Secretary of State in relation to England; the removal of these specific (and uncommenced) powers from all parties is the consequence of the underlying (and uncommenced) duty imposed on undertakers, to which those powers relate, being removed from the 1991 Act by these clauses.

1198 In light of the above, and since the NUAR clauses will therefore alter the executive competence of the Welsh Ministers and the Northern Ireland Executive, the Government considers this to provide a further basis on which the LCM process is engaged.

Registers of Births and Deaths

1199 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.

1200 The clauses which amend the Births and Deaths Registration Act 1953 and the Registration Service Act 1953, relating to the form in which registers are to be kept and the provision of equipment and facilities by local authorities extend and apply to England and Wales only.

1201 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 some of the provisions amended extend to Scotland and Northern Ireland. No LCM is required.

Data protection

1202 The data protection reservations in relation to Scotland, Wales and Northern Ireland apply for the data protection provisions in chapter 1 of Part 5 and provisions in relation to the Information Commission in Part 6 so the LCM procedure is not engaged by these provisions.

Privacy and Electronic Communications

1203 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 LCM is required.

Information standards for health and social care

1204 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 meter communication services

1205 The smart meter communication services measure extends to England, Wales and Scotland only and the subject matter of the Bill is reserved under the Scottish and Welsh devolution settlements. Therefore, an LCM won't be required.

Information to improve public service delivery

1206 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).

1207 There is no relevant reservation for the power in this provision so an 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.

Retention of information by providers of internet services

1208 This provision relates to the reserved matter of internet services and, in Scotland, conferring functions on the Office of Communications. Accordingly, LCMs are not required.

Information for research about online safety matters

1209 These provisions relate to the reserved matter of internet services. Accordingly, LCMs are not required.

Retention of biometric data

1210 These provisions relate to the reserved or excepted matters of national security and, to the relevant extent, counter-terrorism. Accordingly, LCMs are not required.

Trust Services

1211 The technical standards reservation applies in Wales, Scotland and Northern Ireland. An LCM is not required.

Powers relating to verification of identity or status

1212 As the immigration reservation applies in Wales, Scotland and Northern Ireland, no LCM is required for clause 55.

DATA (USE AND ACCESS) BILL [HL]

EXPLANATORY NOTES

These Explanatory Notes relate to the Data (Use and Access) Bill [HL] as introduced in the House of Lords on 23 October 2024 (HL Bill 40).

Ordered by the House of Lords to be printed, 23 October 2024

PUBLISHED BY AUTHORITY OF THE HOUSE OF LORDS