Policy Paper

Data (Use and Access) Bill: European Convention on Human Rights Memorandum

24 October 2024

Summary of the Bill

Part 1: Customer data and business data

This Part:

a. Creates powers to introduce 'smart data' schemes.
b. Includes a power to make regulations requiring suppliers and others to provide customers or authorised intermediaries with customer data and to publish, or provide customers and others with, business data.
c. Supplements this power with powers to make provision to enable or require collection, retention and rectification of data and to allow the exercise of a customer's rights by an intermediary.
d. Supplements this power with powers to make provision requiring suppliers and others to provide data in particular ways, such as via particular interfaces, and to establish and fund a body that can create the standards for this data provision (an "interface body").
e. Further includes powers to make provision about enforcement provisions, the charging of fees and levies and the giving of financial assistance.
f. Creates specific powers for the Treasury to empower the Financial Conduct Authority ("FCA") to oversee smart data schemes in the financial services sector.

Part 2: Digital Verification Services

This Part:

a. Confers on the Secretary of State a duty to prepare and publish a framework setting out rules concerning the provision of digital verification services.

b. Confers a power on the Secretary of State to produce and publish supplementary codes which contain rules concerning the provision of digital verification services which supplement the framework.
c. Confers a duty on the Secretary of State to establish a register of organisations that comply with framework rules and rules which supplement the framework.
d. Contains provision for the governance of this register and related functions.
e. Confers on public authorities a power to disclose information to organisations on this register.
f. Confers a power on the Secretary of State to designate a trust mark for use by registered persons in the course of providing, or offering to provide, digital verification services.
g. Confers a power on the Secretary of State to require information from certain persons where reasonably required for the purposes of the exercise of the Secretary of State's functions under this Part.
h. Confers a power on the Secretary of State to delegate functions under this part to a third party.
i. Amends existing powers to make subordinate legislation in the field of immigration law which will enable the Secretary of State to require employers and landlords who choose to carry out certain digital checks to use the services of organisations registered as complying with designated supplementary rules concerning the provision of those services.

Part 3: National Underground Asset Register

This Part makes amendments to the New Roads and Street Works Act 1991 and the Street Works (Northern Ireland) Order 1995 for the creation of a new legal framework for the National Underground Asset Register ("NUAR").

Part 4: Registers of Births and Deaths

This Part makes amendments to the Births and Deaths Registration Act 1953 enabling registers of births and deaths to be retained in electronic form without the need for a paper duplicate.

Part 5: Data Protection and Privacy

This Part:

a. Amends existing data protection laws to clarify and supplement the definitions of various terms.
b. Enables, by way of regulations, the Secretary of State to add to special categories of personal data and sensitive processing.
c. Reforms provisions relating to automated decision-making.
d. Amends the existing law relating to international transfers of personal data.
e. Brings together safeguards for the processing of personal data for research and related purposes.
f. Exempts the processing of personal data for law enforcement purposes under Part 3 of the Data Protection Act 2018 (the "DPA 2018") from certain requirements where required for reasons of national security.
g. Enables specified joint processing of personal data by an intelligence service and a competent authority to be subject to the same data protection standards (part 4 of the DPA 2018).
h. Makes changes to some of the data protection regulator's enforcement powers and the way in which it carries out its powers and functions.
i. Limits the ability of enactments to override data protection legislation by implication.
j. Makes provision for the making of regulations under the UK GDPR.
k. Makes amendments to the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

Part 6: The Information Commission

This Part changes the constitution of the data protection regulator.

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

This Part:

a. Makes provision about the application, to providers of information technology, of information standards for health and adult social care in England.
b. Makes provision about the process for the grant of a Smart Meter Communication Licence under the Electricity Act 1989 and the Gas Act 1986.
c. Extends the public service delivery information-sharing powers under section 35 of the Digital Economy Act 2017 to improve public service delivery to undertakings.

d. Makes amendments to the Online Safety Act 2023 requiring Ofcom to issue information notices requiring retention of data in certain circumstances.
e. Empowers the Secretary of State to create a regime to allow researchers access to information held by certain providers of internet services, for the purposes of research into online harms
f. Makes amendments to the regime governing the retention by law enforcement authorities of certain biometric data (fingerprints and DNA profiles) for the purposes of national security, permitting retention for longer periods in some circumstances.
g. Makes changes to Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation).

European Convention on Human Rights

Baroness Jones of Whitchurch, Parliamentary Under-Secretary of State for the Future Digital Economy and Online Safety, has made a statement under section 19(1)(a) of the Human Rights Act 1998 that, in her view, the provisions of the Bill are compatible with the Convention rights.

The following section includes an analysis of Convention issues in relation to particular provisions.

Summary of key ECHR issues under the Bill

Part 1:

a. **Regulation-making powers relating to customer data and business data (smart data)** *(clauses 1-24)*: Compliance with Convention rights of regulations under Part 1 (customer data and business data) of the Bill will need to be determined when regulations are made. The Convention rights most likely to be engaged by the regulations are Article 8 and Article 1 of Protocol 1 and, in relation to enforcement of the regulations, Article 6. The Department considers that the clauses contain sufficient requirements and safeguards to ensure compliance with these Articles (see paragraphs 1-24).

Part 2:

a. **Digital Verification Services Register** *(clauses 32-44)*: The Department considers that any interference with rights under Article 1 of Protocol 1 ECHR is justified in the public interest and proportionate (see paragraphs 27-31).
b. **Refusal of an application to or removal from the Digital Verification Services Register** *(clauses 34 and 41)*: The Department considers that this provision complies with Article 6 (see paragraphs 32-34).
c. **Digital Verification Services and data sharing by public authorities** *(clauses 45-49)*: The Department considers that any interference with Article 8 rights pursues a legitimate aim, being in the interests of the economic wellbeing of the country, and is proportionate (see paragraphs 35-39).

Part 3:

a. **Regulation making powers relating to making the information in the National Underground Asset Register available under licence for free or for a charge** (clauses 56-60 and schedules 1 and 2): The Department considers that any interference with rights under Article 1 of Protocol 1 is justified in the public interest and proportionate (see paragraphs 40-43)

Part 5:

b. **Changes to data protection law and Article 8 ECHR**: the Department considers that the changes the Bill makes to data protection law (including those analysed in more detail below) do not give rise to any unlawful interferences with Article 8 rights. The Department has considered both the negative and positive obligations of the State in reaching this assessment (see, in particular, paragraphs 44-51).
c. **Amendments to Article 6 UK GDPR** *(clause 70)*: The Department considers that these provisions are capable of being operated compatibly with Convention rights so that the *Christian Institute* test (see paragraph 55 below) is fulfilled and that it is largely the positive obligation on the State which may give rise to interferences with Article 8 rights. However, the Department considers that this clause does not inhibit the fulfilment of this positive obligation given the margin of appreciation and requirement of reasonable necessity (see paragraphs 52-57).
d. **Searches in response to data subjects' requests** (*clause 78*): The Department considers that any interference with Article 8 rights are justifiable and proportionate (see paragraphs 58-68).

e. **Automated decision-making** *(clause 80)*: The Department considers that any interference with Article 8 rights and Article 14 ECHR (read with Article 8) rights are justifiable and proportionate, given the legitimate aim of ensuring the economic wellbeing of the country and the safeguards which this clause puts in place (see paragraphs 69-82).

f. **National security exemption** *(clause 87)*: The Department considers that any interference with Article 8 rights is justified as in the interests of national security and proportionate (see paragraphs 83-86).

g. **Joint processing by intelligence services and competent authorities** *(clause 88)*: The Department considers that any interference with Article 8 rights is justified as in the interests of national security and proportionate (see paragraphs 87-89).

h. **Interview notices** *(clause 99)* The Department considers that the powers enabling the data protection regulator to compel a person to attend an interview and answer questions are capable of being exercised compatibly with Article 6 ECHR rights (see paragraphs 90-94).

Part 6:

a. **The Information Commission** *(clauses 115-118 and Schedule 14)*: The Department considers that any interference with rights under Article 1 of Protocol 1 is justified in the public interest and proportionate (see paragraphs 95-96).

Part 7:

a. **Information standards for health and social care** *(clause 119 and Schedule 15)*: The Department considers that these provisions comply with Article 6 and that any interference with rights under Article 1 of Protocol 1 is justified in the public interest and proportionate (see paragraphs 97-102).

b. **Retention of information by providers of internet services in connection with the death of a child** (*clause 122*): The Department considers these provisions comply with Article 6, and that any interference with rights under Article 8 and Article 1 of Protocol 1 are justified in the public interest and proportionate (see paragraphs 103-114).

c. **Retention of biometric data for the purposes of national security** (*clauses 124-126*): The Department considers these provisions comply with Article 1 of Protocol 1 and that any interference with rights under Articles 6 and 8 are justified (see paragraphs 115-138)

Customer data and business data (smart data)

1. Part 1 contains regulation-making powers, so the compatibility of any regulations with the Convention rights will need to be determined when those regulations are made. Nonetheless, the Department considers that the clauses in this Part should provide for regulations which are compatible with relevant Convention rights.

2. The principal regulations made under Part 1 will require suppliers of goods, services or digital content specified in the regulations, and other persons who process the relevant data, to provide customers and authorised intermediaries with data relating to that customer ("customer data": clause 2(1)) and/or to publish or provide customers or others (including public authorities, which may then publish the information) with, information relating to the goods, services or digital content supplied ("business data": clause 4(1) and (4)). 'Ancillary' powers may enable or require suppliers to produce, collect and/or retain data (clauses 2(3)(a) and 4(3)) and to rectify inaccurate customer data (clause 2(3)(b)). To allow customers to achieve tangible benefits from access to their data, the regulations may allow an intermediary to take, on the customer's behalf, any action that a customer could take in relation to the goods, services or digital content supplied or provided by the data holder (clause 2(4)): for instance, in a banking context that might include the intermediary accessing the customer's account to make a payment.

3. Part 1 further allows departments or the Treasury to impose specific requirements as to the provision of customer and business data (clauses 3 and 5 illustrate provisions that may be made). This includes the ability to require suppliers and, where appropriate, intermediaries to create, fund and maintain a body to operate an interface for sharing the customer and business data, or to set standards for interfaces run by the suppliers themselves (clause 7).

4. There are also powers for accreditation of intermediaries, including an ability of a decision-maker to suspend or revoke it (clause 7), enforcement powers (clauses 8-10) which are considered in the context of Article 6, and powers to impose fees (clause 11) or a levy (clause 12) to cover costs. For completeness, Part 1 also contains specific powers for the Treasury to empower the FCA to oversee smart data schemes in the financial services sector (clauses 14-17).

5. The principal purpose of the regulations is to enhance data portability rights, and improve their effectiveness, in the specific markets to which regulations will apply. The objective is to tackle information asymmetry between suppliers and their customers to

facilitate better use of customer data, for instance to improve the ability of customers, receiving usable data in 'real time', to compare deals and switch suppliers.

6. The clauses are designed to build on the data portability right under Article 20 UK GDPR but allow provision of data more quickly and in a more usable form than is required under Article 20 and to extend the benefits of data portability to customers which are not individuals, such as small companies. The clauses replace, and improve on, existing regulation-making powers in sections 89-91 of the Enterprise and Regulatory Reform Act 2013 (supply of customer data). The clauses reflect the approach adopted in relation to the open banking scheme and recent powers in Part 4 of the Pension Schemes Act 2021 (which amends the Pensions Act 2004 and the Financial Services and Markets Act 2002) for pensions dashboards.

7. Clauses 2(5) and 4(5)) require that, in deciding whether to make regulations, the Secretary of State or the Treasury must have regard to (inter alia) the likely effects for customers, data holders (including suppliers) and on innovation and competition. Consultation with such persons and regulators as the Secretary of State or the Treasury consider appropriate (clause 22(3) and affirmative Parliamentary scrutiny (clause 22(1)) are both required in the case of the first regulations relating to a particular description of data and for subsequent regulations making requirements more onerous for data holders or interface bodies or which contain provisions under other regulation-making powers in Part 1 which require affirmative scrutiny such as provisions relating to monitoring, enforcement , interface bodies, revenue-raising or under the financial services sector Clauses

Article 8 ECHR

8. Article 8 is potentially relevant to regulations under Part 1 as customer data is likely to be personal data and its collection, use and disclosure may, in principle, constitute interference with respect for private life (Hilton v UK (Application no 12015/86) 57 DR 108).

9. However, the Department considers that regulations are fundamentally designed to improve the ability of customers, or intermediaries authorised by them, to access their data so that customers' data works for them and not against them. Furthermore, customer data is only to be accessed at the request, or with the consent of, the customer. The Department therefore considers that the regulations are unlikely to interfere with privacy and, in any event, the objective of strengthening the position of customers in the relevant market through improved access to data is in the interests

of the economic well-being of the country.

10. Taken as a whole, any regulations will also form part of an evolution of data portability rights established by or under legislation, including Article 20 UK GDPR. They replace existing powers in sections 89-91 of the Enterprise and Regulatory Reform Act 2013 which would not enable smart data schemes with all the features required to be effective.

11. The potential 'ancillary' requirements for suppliers to produce, collect or retain data is justified to ensure that suppliers retain data sets of consistent content and quality, for sufficient time, to allow the 'principal' data access right to be effective.

12. Clause 20(1) provides powers to ensure that the processing of data does not breach obligations of confidence or other processing restrictions. Clause 20(2) provides that regulations are not to be read as authorising or requiring processing of personal data that would contravene data protection legislation and the intention is that the regulations do not displace such data protections. Accordingly, the Department considers that data retention provisions would, for instance, be subject to the right to erasure under Article 17 UK GDPR and indeed clause 2(3)(b) provides powers for customers to request changes to customer data including rectification. Clause 20 mirrors the recently enacted sections inserted in 238B(6) and (7) of the Pensions Act 2004 by the Pension Schemes Act 2021 in relation to pensions dashboards.

13. It is conceivable that suppliers, or connected persons, may themselves be individuals such as in the case of small businesses. However, in such a case, the Department considers it unlikely that regulations would require the disclosure of any data that is sensitive to that individual and again would be in the broader interests of the economic-well-being of customers within the market. In any event, the clauses contain sufficiently broad powers to deal with relevant circumstances or provide for appropriate exemptions or exclusions (see clause 21(1)). Furthermore, the statutory considerations to which the Secretary of State or the Treasury must have regard before making regulations (clauses 2(5) and 4(5)) and requirements of consultation with such persons and regulators as the Secretary of State or the Treasury consider appropriate (clause 22(3)) should also facilitate a proportionate approach in the regulations.

14. Finally, the regulations may contain provision requiring an enforcer to publish information relating to the exercise of decision-making or enforcement functions (clauses 6(9) and 8(5)(c) and (10)). This is intended to allow 'name and shame'

publication of decisions to suspend or revoke accreditation of intermediaries and the imposition of sanctions or convictions. The Department considers it unlikely that such information will fall within the subject matter of Article 8 but even if it does it is justified to incentivise compliance with the scheme and the protection of customer interests through customers being made aware of cases of non-compliance. Furthermore, publication requirements are intended to reflect publication of sanctions by the Information Commissioner under the data protection legislation and the Department for Business and Trade's 'name and shame' publication scheme for breach of national minimum wage legislation.

Article 1 of Protocol 1 ECHR

15. Some or all data held by the supplier, in particular business data may, as an asset of commercial value, be a 'possession'.[1]

16. If Article 1 of Protocol 1 is engaged, it has a wide margin of appreciation and the Department considers that the objectives of improving data portability, and tackling information asymmetry between suppliers and their customers, would justify any interference as being in the general interest. In addition, as already noted, any regulations would form part of a broader evolution of data portability rights, building on the open banking scheme, established by the Competition and Markets Authority by order (the Retail Banking Market Investigation Order 2017).

17. The operation of clauses 3(4), 5(4) and 7 have the potential to affect the financial and human resources of suppliers and intermediaries, particularly in the event that these powers are used to require suppliers or intermediaries to manage and fund an interface body as described in paragraph 3 above.

18. The clauses also contain revenue raising powers to make provision for the payment of fees (clauses 11 and 15(6)) and for a levy (clauses 12 and 16(4)). The purpose of these powers is to ensure that smart data schemes are 'self-funding' and revenue-neutral to the exchequer with all those given functions under Part 1, including enforcers, decision-makers and the FCA when overseeing financial data schemes, able to recover the cost of the performance of their functions. The clauses require clarity as to the amount or the amounts that may be charged, or how they are to be determined and are subject to safeguards in clause 10 and 21(2)-(4) for instance

[1] For instance, goodwill is a possession: *Van Marle v Netherlands* [1986] 8 EHRR 483; *Iatrides v Greece* [2000] 30 EHRR 97.

limiting the discretion that the regulations may confer on a person to set the amount of a penalty or fee or their increase and, in the case of financial penalties, providing procedural safeguards such as mandatory rights of appeal to a court or tribunal. The Department considers that these clauses secure the payment of taxes or other contributions or penalties and are therefore permitted by the second paragraph of Article 1 of Protocol 1.

19. Furthermore, the necessity and proportionality of provisions in regulations should, again, be ensured by the statutory considerations to which the Secretary of State or the Treasury must have regard and by consultation under clause 22(3).

Article 6 ECHR

20. The enforcement provisions of regulations may include the issue and publication of compliance notices (clause 8(5)(a) and (b)) and the imposition of fines and financial penalties (clauses 8(7) and 10) by an enforcer (including the FCA, which has bespoke financial penalty provisions at clauses 16(1) to (3)) and revocation or suspension of the approval of intermediaries who are allowed to act on behalf of the customer (clause 6(4)). Except for the possibility of provision of criminal offences for the provision of false or misleading information and other falsification (clause 8(6)), the enforcement regime is civil, and to be imposed administratively by enforcers, although the imposition of financial penalties (clauses 8(7) and 16(2)) might in substance amount to a quasi-criminal charge.[2] The enforcement powers also reflect section 238G of the Pensions Act 2004 in relation to pensions dashboards which allows regulations to provide for the Pensions Regulator to issue compliance notices and impose financial penalties.

21. The Department again considers that the design of the powers, and constraints they impose, should ensure compatibility with Article 6. The regulations may make provision about the rights of persons affected by the exercise of an enforcer's functions including provision for reviews and appeals (clause 8(8)). However, the regulations must make such provisions where a decision-maker suspends or revokes the ability of an intermediary to receive data (clause 6(7)).

22. The power of enforcers to impose financial penalties is subject to strict requirements in clauses 21(3)-(4) and 10 including as to its procedure which encompass the

[2] Competition and Markets Authority v Flynn Pharma Ltd and another; Competition and Markets Authority v Pfizer Inc and another [2022] UKSC 14 (SC)

opportunity to make representation and a requirement that the regulations contain provision for appeals to a court or tribunal (clause 10(3)).

23. Finally, all regulations containing any provisions relating to enforcement are subject to consultation with such persons and regulators as the Secretary of State or the Treasury consider appropriate and to affirmative Parliamentary scrutiny (clause 22(1)(d) and (3)).

24. The Department submits that all of these provisions, and safeguards, should ensure that the enforcement provision of any regulations will comply with Article 6.

Digital Verification Services

25. Part 2 of the Bill establishes a legislative structure for the provision of digital verification services ("DVS") in the UK, where providers of those services wish to be registered on a government register ("the DVS register"). It also enables public authorities to disclose personal information to registered digital verification services providers ("registered DVS providers") for the purpose of identity and eligibility verification and enables the registered DVS providers to use a trust mark in the course of providing, or offering to provide, the services for which they are registered.

26. In order to become a registered DVS provider and gain access to the information sharing gateway and use of the trust mark, various conditions must be met. For example, the DVS provider must be certified by an accredited conformity assessment body as complying with the DVS trust framework, a document setting out rules concerning the provision of DVS. The Secretary of State has the power to refuse an application to and remove a registered DVS provider from the DVS register where he is satisfied the DVS provider is failing to comply with the DVS trust framework or a supplementary code (relevant only to removal), or where he considers it is necessary in the interests of national security. The Secretary of State also has the power to remove a registered DVS provider from the DVS register where he is satisfied that the provider has failed to provide information under clause 51.

Article 1 of Protocol 1 ECHR

27. Possessions for the purposes of Article 1 of Protocol 1 can include the grant of a licence to carry out a business[3] and termination of a valid licence connected to the carrying out of the underlying business can amount to an interference with Article 1 of

[3] *Megadat.com SRL v. Moldova* (2011).

Protocol 1. The revocation (or change of conditions of licences) affecting the running of businesses can constitute interference by way of a control of use even if a business is able to carry on other activities.[4]

28. The requirement to comply with the DVS trust framework and other requirements in Part 2 has an impact on the way registered DVS providers carry out their business. In addition, there is also a possibility that those organisations providing DVS but who are not registered DVS providers may be impacted because users of DVS may prefer registered DVS providers.

29. The ability to refuse an application to or remove an organisation from the DVS register and the statutory prohibition on the use of the trust mark could amount to an interference by way of control of use of property. However, it would not constitute an interference by way of control of use of property in respect of any future income that could be earned by the organisation from providing digital verification services to a relying party.[5] Article 1 Protocol 1 only applies to existing possessions and is more likely to be engaged where an individual is removed from the DVS register as opposed to a refusal of an application to be added to the DVS register, unless legitimate expectations have arisen[6].

30. Interference with this right can be justified on the basis that it is provided by law; it serves the legitimate public interest of protecting national security and also ensuring that those DVS providers endorsed by the Government, through the DVS register and trust mark, and who can subsequently access personal data of citizens held by public authorities, are complying with the protections and high standards set out in the DVS trust framework and in Part 2 (for example the requirement to have processes and systems in place to ensure the protection and minimisation of personal data) and any relevant supplementary code. The requirements in the legislation are considered a proportionate means of achieving this aim.

31. The power to refuse an application to be added to or to remove an organisation from the DVS Register requires the Secretary of State to be satisfied that the person is failing to comply with the rules of the DVS trust framework or the rules of a supplementary code (relevant only to removal from the DVS register), or the Secretary of State has to consider that it is necessary to refuse an application or remove a DVS

[4] *Bimer SA v Moldova*.
[5] *Ian Edgar [Liverpool] Ltd v the United Kingdom*.
[6] See for example *Pine Valley Developments v Ireland* [1992] 14 EHRR 319

provider from the register in the interests of national security. The Secretary of State can also remove an organisation from the DVS register where he is satisfied that the person has failed to provide information as required under clause 51. This meets the requirements of clarity and foreseeability. There are procedural safeguards that require the Secretary of State to give written notice of an intention to take such action and to afford the organisation the opportunity to make oral or written representations within a specified time-period before refusing an application or removing the organisation from the DVS register.

Article 6 ECHR

32. The Secretary of State will have the power, under clauses 34 and 41, to refuse an application to or remove a DVS provider from the DVS register. The effect of this would be that that DVS provider would be unable to use the trust mark in providing digital verification services and a public authority would not be permitted to disclose information to them under clause 45.

33. While this would not necessarily prevent the DVS provider from providing digital verification services, it may significantly affect business to the extent that the DVS provider relied on public authority information or the recognition of the trust mark. In this respect, and to this degree, inclusion on the DVS register can be seen as akin to a licence, and thus a decision to refuse an application to or remove an organisation from the DVS register under clauses 34 and 41 could amount to the determination of a civil right engaging Article 6 ECHR.[7]

34. While the initial decision would be made by the Secretary of State, who is not an independent judicial body, the Department considers that the availability of judicial review is sufficient to ensure Article 6 compliance. In reaching this conclusion, the Department has considered, in particular, the nature of the decision as administrative, rather than disciplinary, and the procedural safeguards in place to ensure that the decisions under clauses 34 and 41 satisfy fairness requirements. These include requirements for the Secretary of State to give notice stating reasons of his intention to refuse an application or remove an DVS provider from the DVS register and the right for such an organisation to make representations (including, in some cases, the oral representations), unless the Secretary of State is satisfied that stating the reasons would be contrary to the interests of national security. It has been accepted by the

[7] See for example *Tre Traktörer Aktiebolag v. Sweden* (1989).

courts that in a national security context a failure to give reasons may be justified[8], and that executives have a wide degree of discretion in terms of giving reasons for decisions where national security matters arise[9]. As such, it is considered that this limited restriction on the requirement to give reasons under clauses 34 and 41 is justified.

Article 8 ECHR

35. Part 2 of the Bill provides for a power for a public authority to share personal data with a registered DVS provider for the purposes of providing identity and eligibility verification services where an individual has requested those services. The registered DVS provider will be able to use that personal data to build a digital identity and share it with a relying party. A digital identity is based on confirmed identity attributes such as a person's name, age, date of birth, gender, nationality, address, email address, occupation. Identity verification involves a person seeking to prove they are who they say they are, and eligibility verification involves a person seeking to prove they are entitled to a particular service by demonstrating they have a particular attribute. A relying party such as a bank or retailer will be able to ask a registered, trust-marked DVS provider to verify a person's identity or to verify if that person is eligible to do something or use a particular service, for example, open a bank account.

36. The disclosure of personal data by a public authority under this power and the processing of that personal data by registered DVS providers to build a digital identity engages the concept of "*private life*" in Article 8(1) ECHR. However, the Department considers that to the extent this power interferes with the privacy rights in Article 8(1) ECHR, it is justified under Article 8(2). The disclosure is in accordance with the law, pursues a legitimate aim and is necessary in a democratic society.

37. The disclosure of information power in Part 2 is sufficiently clear, precise and foreseeable to meet the "*in accordance with the law*" requirements. Although the power gives a public authority discretion to share personal data with a registered DVS provider, it demarcates the scope of that power. It provides that a public authority can only share information with a DVS provider that has been certified as meeting the technical requirements of the DVS trust framework rules and additionally, where relevant, the rules of a supplementary code. These rules require the DVS provider to be able to demonstrate compliance with the DPA 2018 and the UK GDPR. The DVS

[8] See AF (No3) v Secretary of State for the Home Department [2009] UKHL 28, [2010] 2 AC 269
[9] See Secretary of State for the Home Department v Rehman [2001] UKHL 47 [2003], 26-50

provider also has to be registered by the Secretary of State in the DVS register. The power provides that a public authority can only share information where an individual makes a request to a registered DVS provider for the provision of identity or eligibility services. In practice this means the individual will create an online account with that registered DVS provider through which they will request the registered DVS provider verifies their identity or certain attributes about them against information held by a public authority which can be passed on to the relying party.

38. Public authorities will have to have due regard to a data sharing code of practice, to be laid before Parliament and the first version of which is subject to the affirmative procedure, about the disclosure of information under the power. They will need to be satisfied that the disclosure complies with data protection legislation and ECHR obligations to ensure the security of the data being shared and to safeguard the privacy of individuals. The code will have to be consistent with the code of practice prepared under section 121 DPA 2018 (the data sharing code) and before issuing the code, the Secretary of State will have to consult the Information Commissioner, the devolved administrations and such other persons as the Secretary of State thinks appropriate. There are restrictions on onward disclosure and use of the information shared and the power does not override the protections of the DPA 2018 and the UK GDPR.

39. The measure pursues the legitimate aim of providing individuals with a secure means and confidence to prove things about themselves in a digital environment and for relying parties to be able to trust that proof, in the interest of the economic wellbeing of the country. The measures are proportionate to that aim.[10] Disclosure by public authorities is permitted, not mandated and must comply with data protection legislation. Individuals do not have to use DVS and traditional methods of confirming identity such as passports remain an option for those who wish to use them. The requirements of the DVS trust framework and where relevant, the rules of a supplementary code together with the data sharing code of practice provide sufficient safeguards to minimise the amount of data that is shared and processed to verify a person's identity or confirm a particular attribute, to ensure that the data is accurate, adequate and relevant and not excessive in relation to that purpose, to limit the duration of its storage, to use the data only for the intended purposes and to ensure transparency in relation to the processing.

[10] *Z v Finland*.

National Underground Asset Register

40. The information held by asset owners may have commercial value and therefore, may be considered a "*possession*" for the purposes of Article 1 of Protocol 1 ECHR. The requirements to provide information and make information from the register available to others under a licence (for free or for a charge), could engage Article 1 of Protocol 1 as this could potentially amount to a control and/or deprivation of the use of possessions, depending on the wider circumstances.

41. Insofar as Article 1 of Protocol 1 is engaged, if at all, the Department considers any interference with this right to be justified on the basis that it is lawful, proportionate and in the public interest. Asset owners are already required by law to share information, free of charge, with those having authority to execute street works and those with sufficient interest. This information largely relates to assets laid in the public domain and making this information available is already a requirement for 'safe digging' practices which is in the public interest. The Government has identified significant benefits for the wider economy from the proposed new approach for NUAR, which must be taken into account and weighed against any interference that could arise.

42. Reflecting the approach that already applies in relation to duties set out in section 79 and the (as yet uncommenced) section 80 of the 1991 Act, the core duties of recording information and entering this into NUAR will be enforced by way of criminal offences. The requirements for undertakers to pay fees and provide fee-related information to the Secretary of State will be enforced by way of monetary penalties to be imposed by the Secretary of State. The new Schedule 5A to be inserted into the 1991 Act sets out the procedure that must be followed, including the provision of an initial 'warning notice', and the right to appeal the imposition of a monetary penalty to the First-tier Tribunal, so as to ensure compliance with Article 6 of the Convention.

43. Equivalent provisions have been made for Northern Ireland.

Data protection law and Article 8

44. The protection of personal data is of fundamental importance to a person's enjoyment of the right to respect for private and family life.[11]

45. Some of the changes to data protection laws are therefore likely to engage Article 8. Article 8 is a qualified right, but any interference with it by a public authority must be

[11] (*Satakunnan Markkinapörssi Oy and Satamedia Oy* 95).

"*in accordance with the law*" (Article 8(2)). Relevant legislation must be clear, foreseeable and adequately accessible, necessary in a democratic society and include adequate safeguards to ensure that Article 8 rights are respected.

46. Where this Bill permits data processing which is capable of interfering with Article 8 but does not compel it, the Department does not consider that this will usually be capable of supporting a finding of incompatibility on the grounds of Article 8. See *Christian Institute v Lord Advocate*[12]: "*if a legislative provision is capable of being operated in a manner which is compatible with Convention rights in that it will not give rise to an unjustified interference with Article 8 rights in all or most cases, the legislation itself will not be incompatible with Convention rights*".

47. Where processing is conducted by a public authority and engages a right under the ECHR, that authority must, in accordance with section 6 of the Human Rights Act 1998, ensure that such processing is not incompatible with a convention right. Where processing is conducted by a private body, that processing will not usually engage convention rights.

48. In addition, the State's obligation under Article 8 extends beyond a negative obligation to refrain from action which would interfere with the right to privacy of an individual without proper justification. It is also subject to a positive obligation to ensure respect for private life, including, which might include the adoption of legislation for this purpose[13]. Any system should "*afford the possibility of an effective proportionality assessment of instances of restriction of an individual's rights*". However, there is a margin of appreciation and it is for states to determine how they achieve such protection and the necessary balance between the interests of the individual and the community as a whole.[14]

49. Only in very serious cases will the state have a duty to make specific legislative provision to protect privacy as between private persons (e.g. in the cases of *Söderman v. Sweden*[15] and *K.U. v. Finland*[16], the privacy violations related to child sexual exploitation and abuse).

[12] [2016] UKSC 51, at [94].
[13] See e.g. *Liebsher v Austria* App. No. 5434/17
[14] *ibid*
[15] [GC] (App no. 5786/08)
[16] (2872/02)

50. Having assessed the changes to data protection laws, the Department has not identified any unlawful interferences with Article 8 rights arising from them.

51. However, the Department recognises that there is the possibility that certain changes in particular warrant additional analysis. These are addressed below.

Amendments to Article 6 UK GDPR

52. Article 6(1) UK GDPR sets out the lawful grounds for processing personal data. This forms an element of the 'lawful' requirement for processing personal data in Article 5(1)(a) UK GDPR. The requirement for processing to be 'lawful' in Article 5(1)(a) also means that processing cannot be unlawful for any other reason, including breaching Convention rights.

53. Article 6 UK GDPR sets out a framework that sets out justifications for processing personal data. Not all processing will engage Article 8 ECHR but some will. Article 6(1)(f) is the widest lawful ground and permits processing for any 'legitimate interest' purpose, provided that the "*processing is necessary for those interests, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child*" (the "balancing test"). Clause 70 creates some new lawful bases under a new Article 6(1)(ea) for processing necessary for recognised legitimate interests. These recognised legitimate interests include processing necessary for: making a disclosure in response to a request from a public body or organisation with public functions; national security, public security and defence; detection, investigation and prevention of crime; responding to an emergency; and safeguarding vulnerable individuals. These lawful bases do not incorporate the balancing test that features in Article 6(1)(f) UK GDPR, although they retain the 'necessity' test.

54. The clause also introduces a regulation making power to create further lawful bases, vary existing bases or omit bases added by regulations where the Secretary of State considers it appropriate to do so. Before exercising the power, the Secretary of State will need to decide that it is appropriate to do so, having had regard to the interests, fundamental rights and freedoms of data subjects and 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. The Secretary of State can only add a new basis if it is considered necessary to safeguard an objective listed in Article 23(1)(c) to (j) UK GDPR. There are also consultation requirements to be met before

the power is exercised.

55. New Article 6(1)(ea) will not be available to public bodies processing personal data in the course of their usual tasks and functions. Therefore, in the vast majority of individual cases of processing under that provision, Article 8 ECHR will not apply in any event because the controller is not an emanation of the State. However, there may be a small number of situations in which Article 8 does apply, either because of the unusual nature of the controller, or because of some particular context in which there is a form of positive obligation applicable under Article 8. These cases (so far as they exist) should be comfortably encompassed within the *Christian Institute* test. In other words, when enacted and in force, the new Article 6(1)(ea) may be applied in individual cases in a manner which is incompatible with Article 8 ECHR, but that will be a facet of the individual decision to process personal data on that basis in that context, or in the case of a positive obligation a gap elsewhere in UK law that reveals itself by a specific set of facts, rather than of the existence of Article 6(1)(ea) per se.

56. In addition, in the limited situations in which Article 8 does apply, the new bases will still impose an aspect of any proportionality assessment, namely the requirement of reasonable necessity that the processing is no more intrusive than is required to achieve the specified aim. Save for consent (Article 6(1)(a)), all of the lawful grounds in Article 6(1) UK GDPR impose a necessity test without an additional balancing exercise.

57. The clause (new paragraphs 11 and 12 of Article 6 UK GDPR) also introduces some examples of what may constitute 'legitimate interests' for the purposes of Article 6(1)(f). There is no current indication in the text of Article 6(1)(f) as to what constitutes a 'legitimate interest' but there is an indication in the recitals to the UK GDPR. Paragraphs 11 and 12 incorporate examples from the recitals (recitals 47 to 49) of activities that may constitute a legitimate interest. These are: processing that is necessary for the purposes of direct marketing; intra-group transmission of personal data where necessary for internal administrative purposes and processing necessary for the purposes of ensuring the security of network and information systems. Processing for these purposes will still require both the 'necessity' test and the balancing test in Article 6(1)(f) to be undertaken and therefore the considerations set out above relating to new Article 6(1)(ea) are not relevant.

Searches in response to data subjects' requests

Article 8 ECHR

58. Clause 78 of the Bill amends Article 15 UK GDPR and sections 45 and 94 of the DPA 2018 to codify the principle currently set out in domestic case law that when responding to a request for information and personal data under those provisions a controller is only expected to conduct a reasonable and proportionate search for that information.

59. This provision does not require parties to process information relating to private and family life so does not engage Article 8 directly, but the case law of the European Court of Human Rights ("ECtHR") has established that Article 8 requires that the law must provide an effective and accessible procedure enabling applicants to have access to any important information about them.[17] However, even in those cases the ECtHR has found that there isn't always a right to access the information.

60. The Department is content that the amendment proposed to Article 15 UK GDPR (and the equivalent provisions in Parts 3 and 4 of the DPA 2018) respects Article 8 ECHR, on the basis that Article 8 does not create a right of access to all information, but only to important information. The provision the Department is proposing respects this, as it requires controllers to conduct searches which are proportionate to the request received, such that the more important the information requested is to a data subject, the more detailed the search has to be.

61. Further, as Article 8 is a qualified right, it can be interfered with so long as that interference is in accordance with the law, meets a legitimate aim and is necessary in a democratic society.

62. This clause sets out what is expected of controllers in terms of the search they must undertake when responding to a subject access request, such that any restriction in terms of the search is in accordance with the law.

63. The restriction also meets the legitimate aims of:

    a. balancing a data subject's right to access important information about them and the controller's rights under Article 1 of Protocol 1 ECHR (protection of property which has been interpreted by the ECtHR to encompass businesses' rights to generate income); and

    b. protection of the economic well-being of the country, in that disproportionate expenses (and use of resources) will not have to be incurred by public bodies in conducting unreasonable and disproportionate searches for information

[17] *Youchev v Bulgaria* 12504/09.

requested under a subject access request where the information requested is of limited importance to the data subject.

64. As outlined above, the wording of the provision ensures that any interference is proportionate to the legitimate aims.

65. In addition, data subjects have the right to bring a complaint to the Information Commissioner's Office ("ICO"), or the courts, if they consider that the search conducted by a controller in response to a subject access request was not sufficient. The ICO or the court could review the approach to ensure that the right balance has been struck by the controller, and would have to ensure any decision complied with Article 8 ECHR.

66. These amendments have formal retrospective effect. The ECHR does not create an absolute prohibition on retrospective application of legislation. This provision is codifying the existing legal position as set out in domestic case law in order to avoid legal uncertainty arising following the loss of the general principles of EU law as a result of the REUL Act 2023.

67. The position is, and will continue to be, set out in the ICO's guidance on responding to subject access requests, so it will continue to be clear to controllers what is required of them when responding to such requests, and to data subjects what to expect of a search by a controller.

68. The Department therefore considers these amendments do not create any unfairness and are compatible with the ECHR.

Automated decision-making

69. Clause 80 of the Bill reforms the legal framework governing solely automated decision-making, which can include use of artificial intelligence ("AI"), amending the requirements in Article 22 UK GDPR (which applies to general processing) and sections 49 and 50 of the DPA 2018 (which appliy to processing for law enforcement purposes under Part 3 of the DPA 2018).

70. Article 22 UK GDPR sets out the conditions which apply to limited high-risk AI scenarios 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 instances where necessary for entering into, or the performance of, a contract between a controller and a data subject, or where such activity is authorised

by law, or where a data subject has provided explicit consent.

71. The purpose of this reform is to simplify the automated decision-making regime, achieved by authorising ADM for all purposes - subject to stringent safeguards - whereas before this activity was only permitted where one of three Article 22 bases applied. Article 22B provides restrictions to the new permissive approach, as detailed below. The new Article 22C introduces comprehensive safeguards, resulting in increased transparency and accountability.

72. It is important to note that new Article 22B sets out the general restrictions to Article 22 processing which include (i) processing relying on the new Article 6(1)(ea) as well as (ii) the current restrictions on automated decision-making using special categories of personal data which will remain the same as in the current Article 22(4) i.e. there is no expansion of scope in this regard.

73. The reforms to section 49 and 50 of the DPA 2018 largely mirror the changes being made to Article 22. However, in the law enforcement context the lawful basis for processing is more limited than under the UKGDPR, controllers can only rely on automated decision-making to process personal data where the data subject gives their consent or where the processing is required or authorised by law.

74. Currently controllers processing for law enforcement purposes under Part 3 of the DPA 2018 rarely make use of automated decision-making. The requirement to inform an individual whenever automated decision-making takes place could tip off people that they are subject to investigation. As part of the changes to automated decision-making we are introducing an exemption to the safeguards which will enable the controller to review such a decision after it has been taken, instead of informing the individual at the time, when doing so would, for example, undermine an investigation or jeopardise national security. This change means that the public can continue to have confidence in the automated decision-making process while maintaining operational effectiveness.

75. As a result of the reforms detailed above, it is anticipated that there may be an increase in the number of decisions made using this technology.

76. Article 8 ECHR may be engaged because data subjects may seek to argue that automated decision-making can result in an interference with the right to privacy. Article 14 ECHR provides that the enjoyment of rights and freedoms set forth in the ECHR shall be secured without discrimination on any ground. Any challenge to a breach of Article 14 must be brought in conjunction with another substantive article, in

this case likely to be an interference with Article 8 ECHR. In the automated decision-making context, Article 14 (read with Article 8) may be engaged where this technology is used *and* it has led to bias and discriminatory decisions or outcomes. It is acknowledged that AI systems are capable of reproducing and augmenting the patterns of discriminatory treatment that exist in society. This can occur when the stereotyping biases and blind spots of system developers shape the choices made in the design and deployment of such systems. It can also occur when historical structures of inequality and discrimination become entrenched in the datasets that are used to train AI and machine learning models. become entrenched in the datasets that are used to train AI and machine learning models. It is, however, worth noting that where considering whether there has been meaningful human involvement in the taking of a decision, processing under both UKGDPR and part 3 require a consideration of the extent to which profiling was involved in that decision. Consequently, where a controller takes a decision involving a considerable degree of profiling, they may reasonably be expected to apply the safeguards mentioned above.

77. However, although the reforms to the UK GDPR are likely to increase the level of Article 22 processing undertaken (in particular, by controllers potentially relying on Article 6(1)(f) UK GDPR as noted above), this will be from predominantly private organisations, as public bodies will generally rely on the lawful basis permitted in existing Article 22. The additional processing by private bodies will generally not raise ECHR concerns, because Article 8 ECHR will not be engaged because the controller is not an emanation of the State. However, private sector controllers will be required to consider ECHR rights when carrying out the balancing test required by Article 6(1)(f). The reforms to the DPA 2018 will make it more feasible for public authorities processing for law enforcement purpose to make automated decisions, but the framework continues to benefit from strong safeguards, ensuring any interference with privacy is necessary and proportionate.

78. There is unlikely to be an interference with the State's positive legislative obligation under Article 8 as the as the reforms in clause 80 retain a significant level of protection for privacy and, although Article 6(1)(f) is the widest lawful basis for processing personal data, it nevertheless requires a controller to undertake a balancing test. Article 6(1)(d) UK GDPR is a very limited processing condition and is usually reserved for emergency treatment such as to retain life.

79. Article 8 is a qualified right, and to the extent that there is any interference this can be justified under Article 8(2) if it is prescribed by law, meets a legitimate aim and is

necessary in a democratic society (i.e. it is proportionate). Any interference would be prescribed by law, as would be provided for either in the Bill, or in regulations made under it. The reforms made by this clause to Article 22 UK GDPR pursue a number of legitimate aims including harnessing the benefits of automated decision-making to increase resilience, productivity, growth and innovation across the private and public sectors. The reforms made to the DPA 2018 support the legitimate aims of public safety and preventing disorder or crime.

80. In respect of Article 14 (read with Article 8) although there is a risk that the increase in scope of Article 22 processing could potentially lead to discrimination under Article 14, any application can only be invoked if a situation falls within the ambit of Article 8, which as set out above, will apply in very limited circumstances.

81. Any interference with either the freestanding Article 8 right or Article 14 ECHR (read with Article 8) complies with the principles of necessity and proportionality as the measure has clarified safeguards for data subjects including a requirement on controllers to provide information to the data subject relating to significant decisions based solely on automated processing. Additionally, whilst for Part 3, the controller may apply an exemption to the safeguards, this is in limited circumstances, for example to avoid the obstruction of an investigation or, to protect public or national security and requires the controller to reconsider the decision as soon as is reasonably practical, ensuring there is meaningful human involvement in the reconsideration. New Article 22C and section 50C also enables a data subject to express their point of view with respect to such decisions, to contest them, and to seek human intervention. Furthermore, the reforms seek to enhance fairness, transparency, accountability, for Article 22 processing. These safeguards now apply to all (both private and public) organisations to ensure they are implemented to prevent and minimise harmful outcomes and to facilitate the full enjoyment of the benefits that AI can provide.

82. On this basis, to the extent that these changes to Article 22 UK GDPR and those in part 3 of the DPA 20018 are sufficiently clear to meet the "*in accordance with the law*" requirement, and that the changes to the framework will not give rise to unjustified adverse interferences.

National Security Exemption and Joint Processing by Intelligence Services and Competent Authorities

83. Following engagement with law enforcement agencies and the intelligence services, there are two reforms in the Bill which are being taken forward, which seek to ensure that the law does not inhibit their ability to safeguard national security.

84. The first of these reforms is to introduce a new broad national security exemption in the data protection regime applicable to law enforcement processing (Part 3 of the DPA 2018), replacing the existing more limited national security restrictions**.** This would create broader protections for national security processing in the law enforcement regime, ensuring consistency with the exemptions already available in the other regimes (for example, sections 26 and 110 of the DPA 2018 which provide national security exemptions for processing under the UK GDPR and Part 4 respectively).

85. When applied by controllers, the new national security exemption is likely to involve an interference with individuals' Article 8 rights, as it will enable them to disapply specified data protections rights and obligations to the extent that it is required to safeguard national security.

86. However, such interferences are explicitly permitted by Article 8(2), which provides for interference with these rights where necessary and proportionate for particular purposes, including the safeguarding of national security. Organisations seeking to rely on the national security exemption are required to apply it on a case-by-case basis, ensuring that they carefully consider whether such interferences are required, and only apply the exemption to the extent that it is necessary and proportionate. Furthermore, the new exemption in Part 3 has been drafted to ensure consistency with the existing national security exemptions already available in the DPA 2018 (and the Data Protection Act 1998 previously), which are compliant with the ECHR.

87. The second national security related reform is to permit competent authorities (s.30 and schedule 7 DPA 2018), that have been specified as 'qualified competent authorities' by the Secretary of State, to operate under the intelligence services regime (Part 4 of the DPA 2018) rather than the law enforcement regime when this is required for the purpose of safeguarding national security. The purpose of this proposal is to simplify data protection considerations by enabling a single set of data protection rules to apply to joint processing activity by the law enforcement and intelligence services, which is judged to have significant operational benefits, enabling closer working in efforts to detect and combat national security threats.

88. Broadening the scope of the Part 4 regime to facilitate joint processing between law enforcement and intelligence services may interfere with individuals' Article 8 rights,

as any processing of their personal data covered by a designation notice will be governed by the intelligence services regime in Part 4, rather than the law enforcement regime in Part 3. Part 4 applies different standards and obligations, appropriate to national security related processing.

89. Nevertheless, that regime still provides data subject rights, principles and obligations to ensure that even data processed by the intelligence services is subject to robust safeguards. The Part 4 regime was designed to specifically address the challenges of processing in a national security context while still ensuring compliance with both Article 8 ECHR and the modernised Convention 108. Any processing by the qualified competent authorities, under Part 4, will apply the same high standards and as a result the reforms moving processing to Part 4 are consistent with the requirements of Article 8 ECHR. Furthermore, these reforms have been designed to limit the impact on individuals, with the requirement to have a notice in place ensuring that designation notices are only used where the processing is required for the purpose of safeguarding national security. The involvement of the ICO in the decision process also ensure significant independent scrutiny.

Interview notices

90. Clause 99 enables the Information Commissioner, as the data protection regulator, to issue a notice compelling a person to attend an interview at a time and place identified by the Commissioner and to answer questions for the purposes of investigating a suspected failure or offence under data protection legislation. The Commissioner will be able to issue an interview notice to the controller or processor, a current or former employee of the controller or processor or any person who was at any time concerned in the management or control of the processor, for example an external consultant. Failure to comply with an interview notice can result in a monetary penalty. It will be a criminal offence to knowingly or recklessly make a false statement in response to an interview notice punishable by a fine. Given the coercive nature of the power, it has the potential to interfere with the privilege against self-incrimination which is an essential part of the right to a fair trial as protected by Article 6 ECHR.[18] The Department considers there are sufficiently robust safeguards and restrictions to prevent the power being used in a way that would infringe the privilege against self-incrimination and that the provisions are compatible with Article 6.

[18] *Saunders v UK* 43/1994/490/572

91. The requirement for an individual to attend an interview and to answer questions must be contained within a written notice which sets out the nature of the suspected failure or offence that is being investigated, provides information about the consequences of failure to comply with the notice and provides information about rights of appeal to the Tribunal against the notice. Where the interview notice is issued on an urgent basis, it must set out the Commissioner's reasons for reaching that opinion. The notice cannot require a person to attend an interview before the end of the period for bringing an appeal (except where the notice is issued on an urgent basis in which case the period is shortened). When a person brings an appeal, they will not be required to attend the interview until the appeal is determined or withdrawn. The Information Commissioner will be required to publish regulatory guidance about the exercise of its functions in connection with this power. Furthermore, the decision to issue an interview notice is subject to the Information Commissioner's duty to have due regard to the principle that regulatory activities should be carried out in a proportionate manner under section 21 of the Legislative and Regulatory Reform Act 2006. These safeguards will enable an individual to challenge an improper request to attend an interview and answer questions. It is envisaged that the power will be used in a minority of investigations where the nature of the data processing and the corporate structure of the organisation is particularly complex; where there is a risk that evidence could be destroyed; where there is an ongoing or increased risk of harm to data subjects.

92. The Department considers that in order to meet its statutory obligations to monitor and enforce data protection compliance, there are strong public interest grounds for the Commissioner having appropriate investigatory powers that make it possible to establish a detailed understanding of a suspected failure or offence under data protection legislation. The safeguards and restrictions that the power is subject to and the existence of other investigatory powers ensure that a proper balance is struck between the public interest, the availability of less intrusive means for obtaining the information required and the individual's interests. The intention is that information obtained under this power will support expedited investigations and will furnish the Commissioner with a more robust and detailed understanding of any suspected failure or offence. It will also assist the Commissioner to form a correct and accurate interpretation of additional evidence obtained through other investigatory powers.

93. The power will be subject to the same restrictions that apply to the Commissioner's existing investigatory powers for Assessment Notices and Information Notices. The Information Commissioner cannot compel a person to answer questions if requiring

them to do so would infringe parliamentary privilege, infringe legal professional privilege or, would reveal evidence of the commission of an offence and expose the person to proceedings for that offence, with the exception of offences under data protection legislation and the offences specified in the clause.

94. As is the case for Information Notices, there will be restrictions on the use which may be made of a statement made or an answer given in an interview. Such statements or answers cannot used be used in evidence against the person on a prosecution for an offence under data protection legislation (except for the offences of knowingly or recklessly making a false statement) unless the person says something in evidence which is inconsistent with their statement or answer in the interview and, if evidence relating to what the person said in interview is adduced, or a question relating to it is asked by or on behalf of that person. This ensures that the information obtained from a compulsory interview can only be used against that individual in a prosecution under data protection legislation in limited circumstances. To the extent that any further interference may arise on a prosecution for an offence under data protection legislation or other offences, it would be open to a trial judge to exclude any unfair evidence under section 78 Police and Criminal Evidence Act 1984 to ensure the fairness of the proceedings.

The Information Commission

95. The Bill abolishes the office of the Information Commissioner (which is presently constituted as a corporation sole), and replaces it with a new board of directors, comprised of a chair, chief executive and board members, with the current functions of the Information Commissioner being discharged by the board of the new body, the Information Commission, rather than being vested in and formally discharged by the Information Commissioner, as at present. The new model provides an oversight and supervisory function, which is considered best practice not only for regulatory bodies, but public and private sector organisations alike.

96. The Bill provides (via transitional provision in Schedule 14) that the Information Commissioner is transitioned into the role of chair of the board of the new body, for a term that expires at the time that the Information Commissioner would have ceased to hold office but for the abolition of the role under the Bill. The Department considers that the abolition of the office of Information Commissioner by the Bill is compatible with Article 1 of Protocol 1 ECHR: there's a strong rationale for the changes made in the Bill and, on the basis that the Information Commissioner will be appointed to the

new body on the same salary and pension entitlements as under the original appointment, and for the same term, the Information Commissioner's tenure and remuneration package will be protected.

Information standards for health and adult social care

Article 6 ECHR

97. Decisions concerning the imposition of information standards, the accreditation scheme, or the enforcement of the measure (via monitoring, compliance requests, financial penalties and a power for the Secretary of State, if they have reasonable grounds to suspect that an information technology provider is not complying with an information standard, to publish a statement to that effect ("public censure provision")) could engage Article 6 insofar as they could involve administrative determinations of the civil rights of information technology providers.

98. Article 6 provides that everyone, in the determination of their civil rights and obligations or of any criminal charge against them, is entitled to a fair and public hearing. The Department considers that the decisions in question, for example to publish binding information standards on information technology providers are properly characterised as an exercise of administrative discretion, and therefore that they are comfortably amenable to judicial review. When taken in the context of the recognised freedom of the state in administrative policy-related decision-making, the ability of the court to consider whether the Secretary of State is acting within their powers when imposing requirements and to apply other general principles of judicial review is considered to be sufficient to satisfy the requirements of Article 6.

99. The powers are thus capable of being exercised compatibly with Article 6. This includes the level of financial penalties which will be set out in (or determined in accordance with) regulations and which would be set proportionately and in relation to which the provider would have an opportunity to make representations, and the public censure provisions under which the provider must be given an opportunity to make representations. Further where appropriate, the provisions would trigger provisions about appeals to independent bodies (the First-Tier tribunal). In summary, the Department is of the opinion that the provisions are compatible with Article 6, as the requirements of this Article are largely met by the ability of providers to challenge the Secretary of State's decisions by way of judicial review and/or before a tribunal.

Article 1 of Protocol 1 ECHR

100. The Department considers that the imposition of information standards or the enforcement of the measure (via monitoring, compliance requests, financial penalties and the public censure provision) could engage Article 1 of Protocol 1 insofar as they could affect the carrying on by information technology providers of private commercial activities.

101. Article 1 of Protocol 1 is a qualified right and any interference can be justified if it is in the public interest and subject to the conditions provided for by law and by the general principles of international law. The Article does not impair the right of the state to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure payment of taxes or other contributions or penalties. The provisions pursue a number of legitimate aims including improving the flow of health and care information and to bring individuals closer to their data by enabling easy access, in real time, to all the health and/or social care information relevant to care. These can effectively be achieved through uniformity as regards the systems used to record information and this necessarily requires the imposition of standards in respect of the design or other characteristics of the information technology and information technology services supplied by IT providers.

102. The standards would be limited to those which are necessary to achieve these aims and the powers are capable of being exercised compatibly with the ECHR. This includes the level of financial penalties which will be set out in (or determined in accordance with) regulations and which would be set proportionately and in relation to which the provider would have an opportunity to make representations, and the public censure provisions under which the provider must be given an opportunity to make representations. Further, the exercise of the powers would be amenable to judicial review and, where appropriate, would trigger provisions about appeals to independent bodies (the First-Tier tribunal). The Department therefore considers the provisions to be compatible with Article 1 of Protocol 1.

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

Article 8 ECHR

103. Clause 122 amends section 101 of the Online Safety Act 2023 (and other related sections) 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 specific kinds of regulated service providers requiring them to retain certain information

relating to the use of the service by the deceased child for a specified period. It also gives OFCOM a power to serve a notice on a "*relevant person*" as defined in section 101 of the Online Safety Act 2023 to ensure the retention of information relating to the use of a relevant regulated service.

104. The provision does not provide OFCOM with a power to require disclosure of the information, nor does the provision itself create a requirement for the parties to retain data. Instead, the provision gives OFCOM a duty to issue notices requiring retention of the data in case it is later required in order to respond to a notice under section 101(1) of or Schedule 5 to the Coroners and Justice Act 2009, Coroners Act (Northern Ireland) 1959 or the Fatal Accidents and Sudden Deaths etc. (Scotland) Act 2016.

105. The processing carried out by recipients of these notices are private bodies, and not emanations of the state, and so Article 8 will not be engaged by those bodies retaining the information. Further, much of the information likely to be caught by this provision will not fall within Article 8, as it is focused on data relating to the deceased child's use of an online service.

106. The provision is unlikely to constitute an interference with the State's positive legislative obligation under Article 8 to ensure respect for private life, as the provision contains numerous safeguards intended to ensure protection for privacy.

107. Article 8 is a qualified right, and to the extent there is any interference this can be justified under Article 8(2) if it is prescribed by law, meets a legitimate aim and is necessary in a democratic society (i.e. is proportionate). Any interference in this case would be prescribed by law, as it would be provided for by the provision in the Bill. The provision serves the legitimate public interests of protecting public health and morals, prevention of crime and for the protection of rights and freedoms of others, namely ensuring that coroners and procurators fiscal can properly investigate the circumstances surrounding a child's death, and the provision is a proportionate way of achieving those aims.

108. This clause is sufficiently clear, precise and foreseeable to meet the "*in accordance with the law*" requirements. Although the provision does not create the obligation to retain the information in question, it creates a duty on OFCOM to issue notices requiring such retention, and the provision clearly sets out the circumstances in which such a notice might be issued. It makes it clear that a notice can only be given

where the Coroner or Procurator Fiscal notifies OFCOM of a child death , and so ensures this process is focused on the cases where it has been shown there was an issue with the current process.

109. The kinds of regulated services, providers of which are to be given the notices, are to be set out in regulations made by the Secretary of State, and when making those regulations the Secretary of State will need to ensure a proportionate approach has been adopted to naming the kinds of regulated services caught by this provision. The Coroner or Procurator Fiscal is able to ask for OFCOM to issue notices in relation to additional regulated services specifically drawn to their attention, again ensuring proportionality.

110. The provision makes it clear what types of data could be caught, that it is only information relating to the deceased child's use of the named service which should be held, and sets out a clear process for ensuring that the information is not retained for longer than required.

111. The provision also makes it clear that the processing required under a notice issued by OFCOM must (where it involves third party personal data) comply with the data protection legislation, thus ensuring that appropriate protections remain in place for third parties whose data may be caught, for example that the data retained cannot then be processed in other ways which would not be permitted under the data protection legislation.

112. In addition, as decisions made in connection with this provision will be made by public authorities under the Human Rights Act 1998, they will be under a duty to act compatibly with the ECHR and any decisions can be subject to judicial review, providing a further safeguard.

Article 1 of Protocol 1 ECHR

113. As the provision requires certain regulated service providers to search for, retain and respond to OFCOM confirming steps taken to comply with the information notice, this provision may engage Article 1 of Protocol 1 on the basis it restricts providers' ability to delete information and will incur some costs in complying with the provision. However, the Department is content that any interference with this right is lawful in that it is in the general interest for the reasons set out in respect of Article 8 above.

Article 6 ECHR

114. This provision applies the enforcement provisions relating to information notices under the Online Safety Act 2023 to failures to comply with the requirements under an information notice issued under this provision[19] and creates a limited number of criminal offences tailored to this new type of information notice. The Department considers there are sufficiently robust safeguards and restrictions in place to prevent the enforcement provisions being used in a way that would offend the protection against self-incrimination and Article 6.

Retention of biometric data for the purposes of national security

115. Clauses 124-126 make amendments to the regime governing the retention by law enforcement authorities ("LEA") of certain biometric data (fingerprints and DNA profiles) for the purposes of national security, under sections 18 to 18E of the Counter-Terrorism Act 2008 ("CTA 2008").

116. The amendments, which are summarised below, are considered to be compatible with the Convention rights of persons whose biometric data will be affected. In summary, the effect of the amendments is as follows:

a. Recordable offences (clause 124): this clause will enable LEAs to retain the biometric data, potentially indefinitely, of persons who have convictions for offences in other jurisdictions that are equivalent to recordable offences in England and Wales or Northern Ireland;

b. Pseudonymised data (clause 125): this clause will enable LEAs to retain biometric data, potentially indefinitely, that has been supplied by an overseas law enforcement authority in an identifiable form, if the UK authority takes steps to 'pseudonymise' it (i.e. ensure it is held in a way which does not identify the individual) as soon as possible after receipt;

c. INTERPOL data (clause 126): this clause will enable LEAs to retain biometric data obtained as part of a request for co-operation or a threat notification that has been sent by INTERPOL, for so long as the request or the threat notification remains outstanding.

[19] The detailed analysis of these provisions can be seen in paragraphs 76-84 of the ECHR Memorandum for the Online Safety Bill.

117. These clauses also make retrospective provision to enable the ongoing retention and use of certain biometric data being held by LEAs on the date of commencement, that would otherwise fall to be destroyed.

118. It is accepted that all three clauses involve at least a potential interference with the Article 8 rights of persons whose biometric data will be affected.

Recordable offences (clause 124): Article 8 ECHR

119. The interference with Article 8 rights is in accordance with the law (the retention being authorised by these amendments to the CTA 2008) and is justified by the need to safeguard national security. The interference is also assessed to be a proportionate means of achieving that aim.

120. In *Gaughran*[20] the ECtHR found that the indefinite retention (in Northern Ireland) of biometric data relating to persons who had convictions for recordable offences was not a proportionate means of achieving the legitimate aim of the prevention of crime. In reaching this conclusion, the Court emphasised the following:

a. The biometric data was retained without any consideration of the seriousness of the offence for which the individual was convicted;

b. The retention regime did not require periodic assessment as to whether there was a continuing need to retain the data indefinitely; and

c. The retention regime did not include any mechanism by which the individual could seek to have the data deleted.

121. The Court was considering the regime that existed prior to the enactment of Part 3 of the DPA 2018. The Department considers that the requirements that arise under that Part provide sufficient additional safeguards to render proportionate a regime allowing for the possibility of indefinite retention of data that relates to persons with convictions for recordable offences (and now for offences in other jurisdictions that are equivalent to recordable offences).

122. In particular, the fifth data protection principle requires a law enforcement authority to process biometric data only for as long as is necessary to achieve the purposes for which it is retained; and to conduct appropriate periodic reviews of the

[20] *Gaughran v UK* (App no. 4245/15).

necessity of ongoing retention. Chapter 3 of Part 3 of the DPA 2018 confers a right to seek the erasure of biometric material, and the right to complain to the Information Commissioner.

Pseudonymised data (clause 125): Article 8 ECHR

123. In the Department's view it is unlikely that a court would find that the retention of the biometric data in a pseudonymised form amounts to an interference with the Article 8 rights of the persons concerned, given that the clause will authorise the retention of material only if the LEA has taken the required steps to retain it in a form that does not enable the authority to know the person's identity.

124. However, to the extent that there is an interference, it is in accordance with the law and is justified by the need to safeguard national security.

125. In addition, the retention is a proportionate means of achieving that aim. The interference with Article 8 rights is considerably reduced in circumstances where the law enforcement authority does not know the identity of the person whose data is being processed. That interference is outweighed by the potential benefits to national security of the LEA having access to this information. In order to retain the biometric material, the authority will also have to comply with the requirements under the DPA 2018.

126. Where the law enforcement authority comes to know the identity of an individual, for example through a match with a visa application, the biometric data would then need to be managed under existing provisions of the CTA. Specifically, a three year retention period would apply from the point of identification, which is considered to be a proportionate period given the operational value of this information to national security.

INTERPOL data (clause 126): Article 8 ECHR

127. The interference with Article 8 rights is in accordance with the law, is justified by the need to protect national security, and is a proportionate means of achieving that aim.

In accordance with the law

128. The additional interference will be provided for by amendments made to the section 18 retention regime by this Bill and will therefore be in accordance with the law.

129. The period for which a law enforcement authority will be permitted to retain the biometric material will be tied to period for which the INTERPOL notice remains in force. The Department considers that the INTERPOL data processing regime meets the 'quality of law' requirements, as it imposes adequate legal protection against arbitrariness and will enable persons to understand the circumstances in which a LEA will permitted to retain, or required to destroy, their biometric data.

130. In addition, in processing this biometric data, law enforcement authorities will have to meet their relevant obligations that arise under Part 3 of the DPA 2018.

Proportionality

131. The Department considers that the interference is a proportionate means of safeguarding national security.

132. The ECtHR has held in the past that a regime that allows for the general indefinite retention of biometric data is unlikely to be proportionate.[21] To meet the requirement of proportionality, the relevant regime should ensure that the processing of biometric data is not excessive in relation to the purposes for which it is retained; and retained for no longer than is required for the purpose for which it is stored.[22]

133. The measure will authorise the retention of data only for so long as the relevant INTERPOL notice remains in force. The INTERPOL data protection regime imposes various requirements surrounding notices; including a requirement that there be periodic assessment as to whether various conditions relating to the notice are satisfied, and that such periodic assessment take place at least once every 5 years. If the assessment is that there is no longer a need for the notice to have effect, it will be cancelled, and any biometric data that is linked to it will have to be destroyed.

<u>Retrospective provision: Article 6 and Article 1 of Protocol 1 ECHR</u>

134. These clauses make retrospective provision to authorise the retention and use of certain legacy data that an LEA was required to destroy prior to the date of commencement of the clauses (i.e. as if the relevant destruction requirement had never arisen).

135. There is a possibility that this provision could constitute an interference with the

[21] *S v UK* 48 EHRR 50 ("*Marper*"), paragraph 125.
[22] See *Marper*, paragraph 103.

Article 6 rights of a person who brought a claim in respect of the unlawful retention of their data prior to the commencement of the clauses (although no such litigation has been brought to date). To the extent that there is any such interference, it will be justified and proportionate for the reasons that are set out above.

136. The retrospective provision does not engage the 'Zielinski principle'[23] (which prohibits, as contrary to Article 6 ECHR, retrospective legislation that is intended to alter the outcome of pending litigation). These clauses are of general application and are intended to further the protection of national security by allowing valuable national security-related data to be retained and used (if in accordance with the DPA 2018).

137. In addition, the formally retrospective provisions do not involve any interference with the right to peaceful enjoyment of possessions under Article 1 of Protocol 1. It is well-established that for a claim to amount to a possession, it must have a clear basis in law[24]; and a potential claim that has yet to be issued is unlikely to be sufficient.

138. To the extent that these clauses do involve a deprivation of a property right, that deprivation is in accordance with the law, is justified and is proportionate for the reasons given above.

The Department for Science, Innovation and Technology, the Home Office, the Department for Business and Trade, HM Treasury and the Department of Health and Social Care.

[23] *Zielinski v France* 31 E.H.R.R. 19.
[24] See *Kopecky v Slovakia* 41 E.H.R.R. 43.