Policy Paper

Data Protection and Digital Information (No. 2) Bill: European Convention on Human Rights Memorandum

8 March 2023

Summary of the Bill

Part 1: Data Protection

This Part:

a. Amends existing data protection laws to clarify and supplement the definitions of various terms.
b. Introduces a new lawful ground for processing personal data.
c. Makes changes relating to data subjects' rights to access their personal data.
d. Reforms provisions relating to automated decision making.
e. Makes changes to the obligations of data controllers and processors.
f. Amends the existing law relating to international transfers of personal data.
g. Brings together safeguards for the processing of personal data for research and related purposes.
h. Exempts the processing of personal data for law enforcement purposes under Part 3 of the DPA 2018 from certain requirements where required for reasons of national security.
i. 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).
j. Makes changes to some of the data protection regulator's enforcement powers and the way in which it carries out its powers and functions.
k. Limits the ability of enactments to override data protection legislation by implication.
l. Makes provision for the making of regulations under UK GDPR.

Part 2: Digital Verification Services

This Part:

a. Confers on the Secretary of State a duty to prepare and publish a framework relating to the provision of digital verification services.
b. Requires the Secretary of State to establish a register of organisations that comply with such a framework.
c. Contains provision for the governance of this register and related functions.
d. Confers on public authorities a power to disclose information to organisations on this register.

Part 3: Customer data and business data

This Part:

a. Creates powers to introduce “smart data” schemes in specific markets.
b. Includes a power to require suppliers and others to provide customers with customer data and business data.
c. Supplements this power with powers to require collection, retention and rectification of data and to allow the exercise of a customer’s rights by an intermediary.
d. Further includes powers to create enforcement provisions, to charge fees and a levy and give financial assistance.

Part 4: Other provision about digital information

This Part:

a. Makes amendments to the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).
b. Makes changes to Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation).
c. Extends the public service delivery information-sharing powers under s 35 of the Digital Economy Act 2017 to improve public service delivery to undertakings.
d. Enables the implementation of future international agreements on sharing information for law enforcement purposes.

e. Makes amendments to the Births and Deaths Registration Act 1953 enabling registers of births and deaths to be retained in electronic form.
f. Makes provision about the application, to providers of information technology, of information standards for health and adult social care in England.

Part 5: Regulation and Oversight

This Part:

a. Changes the constitution of the data protection regulator.
b. Makes changes to the oversight of biometric data.

European Convention on Human Rights

The Secretary of State 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, on introduction of the Bill in the House of Commons.

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. **Changes to data protection law and Article 8:** 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, paras 1-8).
b. **Amendments to Article 6 UK GDPR** *(clause 5*): The Department considers that these provisions are capable of being operated compatibly with Convention rights so that the *Christian Institute* test (see paragraph 3 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 paras 9 - 14).

c. **Automated decision-making** *(clause 11)*: The Department considers that any interference with Article 8 rights and Article 14 (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 clause 11 puts in place (see paras 15-27).
d. **National security exemption** *(clause 24)*: The Department considers that any interference with Article 8 rights is justified as in the interests of national security and proportionate (see paras 28-34).
e. **Joint processing by intelligence services and competent authorities** *(clause 25)*: The Department considers that any interference with Article 8 rights is justified as in the interests of national security and proportionate (see paras 28-34).
f. **Interview notices** *(clause 36)* 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 rights (see paras 35-39).

Part 2:

a. **Digital Verification Services Register** *(clauses 48-53)*: The Department considers that any interference with rights under Article 1 of Protocol 1 is justified in the public interest and proportionate (see paras 40-44).
b. **Removal from the Digital Verification Services Register** *(clause 52)*: The Department considers that this provision complies with Article 6 (see paras 45-47).
c. **Digital Verification Services and data sharing by public authorities** *(clauses 54-56)*: 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 paras 48-52).

Part 3:

a. **Regulation-making powers relating to customer data and business data (smart data)** *(clauses 61-77)*: Compliance with Convention rights of regulations under Part 3 (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 paras 53-73)

Part 4:

a. **Information standards for health and social care** *(clause 99 and Schedule 12)*: 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 paras 74-79).

Part 5:

a. **The Information Commission** *(clauses 100-102 and Schedule 13)*: The Department considers that any interference with rights under Article 1 of Protocol 1 is justified in the public interest and proportionate (see paras 80-81).

Preliminary: Data protection law and Article 8

1. The protection of personal data is of fundamental importance to a person's enjoyment of the right to respect for private and family life (*Satakunnan Markkinapörss Oy and Satamedia Oy v. Finland 2017*).[1]

2. 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 "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.

3. 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* [2016] UKSC 51; (2017) SC (UKSC) 29 at [94]: "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

[1] (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC], 2017*, § 137; *Z v. Finland, 1997*, § 95).

Article 8 rights in all or most cases, the legislation itself will not be incompatible with Convention rights."

4. Where processing is conducted by a public authority and engages a right under the ECHR, that authority must, in accordance with s 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.

5. 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 (see e.g. *Liebsher v Austria* App. No. 5434/17). 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 (*ibid*.).

6. 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* [GC] (App no. 5786/08) and *K.U. v. Finland* (2872/02), the privacy violations related to child sexual exploitation and abuse).

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

8. 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

9. 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 ECHR Convention Rights.

10. 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 5 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: national security, public security and defence; detection, investigation and prevention of crime; responding to an emergency; safeguarding vulnerable individuals and for democratic engagement. These lawful bases do not incorporate the 'balancing test' that features in Article 6(1)(f) UK GDPR, although they retain the "necessity" test.

11. The clause also introduces a regulation making power to create further lawful bases where the Secretary of State considers it appropriate to do so. When creating any further lawful bases, the Secretary of State will need to consider the interests, fundamental rights and freedoms of state subjects and the need to provide children with special protection where relevant.

12. 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.

13. In addition, in the limited situations in which Article 8 does apply, the new legal 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.

14. The clause (new paras 9 and 10 of Article 6(1)(f) 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 (9) and (10) bring 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.

Automated individual decision-making, including profiling: Article 8 and the combined effect of Article 8 and Article 14

15. Clause 11 of the Bill reforms the legal framework governing solely automated decision-making, which can include use of artificial intelligence, amending the requirements in Article 22 of the UK GDPR (which applies to general processing) and sections 49 and 50 of the DPA 2018 (which applies to processing for law enforcement purposes under Part 3 of the DPA 2018).

16. Article 22 of the UK GDPR sets out the conditions which apply to limited high-risk Artificial Intelligence 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 required by law, or where a data subject has provided explicit consent. Clause 11 expands the scope of the existing Article 22 to include the following lawful bases for processing personal data:

(i) Article 6(1)(d) UK GDPR - processing is necessary in order to protect the

vital interests of the data subject and

(ii) Article 6(1)(f) UK GDPR - where the processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which requires protection of personal data, in particular where the data subject is a child" (the 'balancing test').

17. The purpose of this reform is to simplify the data protection considerations so that all automated decision-making within scope of personal data in new Article 22A and sensitive personal data as set out in new Article 22B is permitted, but all such processing is now subject to the same comprehensive safeguards found in new Article 22C resulting in increased transparency and accountability.

18. 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 (ii) as 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.

19. 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, 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 (so the scope is more limited than under the UK GDPR). Currently controllers processing for law enforcement purposes under Part 3 of the DPA rarely make use of automated processing. However, one of the reforms being made will make it more possible for the police and others to use this technology. Currently the requirement to inform an individual whenever automated decision-making takes places limits operational usefulness, as it could tip off people that they are subject to investigation. These reforms 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. This change means that individuals can continue to have confidence in the automated decision-making process while maintaining operational effectiveness.

20. As a result of the reforms detailed above, it is anticipated that the changes to the

rules governing automated decision-making may increase the number of decisions made using this technology.

21. 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 of the 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 ECHR (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 AI 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.

22. However, although the reforms to the UK GDPR are likely to increase the level of Article 22 processing undertaken, 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. 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

23. There is unlikely to be an interference with the State's positive legislative obligation under Article 8 as the as the reforms in clause 11 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.

24. 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 of the 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.

25. 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.

26. 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 bolstered safeguards for data subjects including a requirement on controllers to provide information to the data subject relating to significant decisions being taken through solely automated processing. 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.

27. On this basis, to the extent that these changes to Article 22 UK GDPR 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

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

29. 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), 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, section 26 of the DPA 2018 provides a national security exemption applicable to the UK GDPR).

30. When applied by data 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 necessary to safeguard national security.

31. 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 and only apply the exemption to the extent that it is necessary. 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 DPA 1998 previously), which are compliant with the ECHR.

32. The second national security related reform is to extend the scope of the data protection regime applicable to data processing by the intelligence services (Part 4 of the DPA). This reform will permit specified law enforcement agencies to operate under the intelligence services regime in limited circumstances (rather than the law enforcement regime). 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 police and intelligence services, which is judged to have significant operational benefits, enabling closer working in efforts to detect and combat national security threats.

33. Broadening the scope of the Part 4 regime to cover additional processing by the police 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, reflecting the fact that it applies to extremely sensitive national security related processing.

34. 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 of the ECHR and the modernised Convention 108. Any processing by the police under Part 4 will apply the same high standards and as a result the reforms moving process to Part 4 are consistent with the requirements of Article 8 of the ECHR. Furthermore, these reforms have been designed to limit the impact on individuals, with the requirement to have a notice in place ensuring that these changes will only apply to specific operations/projects where national security is engaged. The involvement of the ICO in the decision process also ensure significant independent scrutiny.

Interview notices

35. Clause 36 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 data controller or processor, a current or former employee of the data 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 of the ECHR (*Saunders v UK* 43/1994/490/572). 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 of the ECHR.

36. 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.

37. 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.

38. 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.

39. 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.

Digital Verification Services Register

40. The technical requirements and standards of the verification services trust framework rules, the certification of digital identity organisations by accredited conformity assessment bodies, the registration requirements and the designation of a trust mark engage Article 1 Protocol 1 as they could impact the ability of registered organisations to provide identity verification and eligibility services.

41. Possessions for the purposes of Article 1 Protocol 1 can include the grant of a licence to carry out a business (*Megadat.com SRL v. Moldova (2011)*) and termination of a valid licence connected to the carrying out of the underlying business can amount to an interference with Article 1 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 *(Bimer SA v Moldova)*. The ability to suspend or remove an organisation from the 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, although not in relation to any future income that could be earned by the organisation from providing digital verification services to a relying party (*Ian Edgar [Liverpool] Ltd v the United Kingdom*).

42. Interference with this right can be justified on the basis that it is provided by law; it serves the legitimate public interest of ensuring that public authorities do not disclose

the personal data of citizens to organisations who are failing to meet their obligation of having a certificate confirming that they are providing digital verification services in accordance with the trust framework in order to be registered by the Secretary of State. These are proportionate measures for organisations who wish to provide digital verification services based on trusted data sets held by public authorities.

43. The power to remove or suspend an organisation from the register requiring the Secretary of State to be satisfied the organisation is failing to provide verification services in accordance with the verification services trust framework, 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 removing the organisation from the register.

44. If removal of an organisation from the register amounts to interference by way of a control of use because it would have the immediate effect of preventing the organisation from providing verification services, the Department considers the interference serves the legitimate public interest and is proportionate. It pursues the legitimate aim of ensuring individuals have a secure means of proving things about themselves in a digital environment by ensuring that digital verification services can only be provided by organisations able to demonstrate compliance with the trust framework including a requirement to have processes and systems in place to ensure the protection and minimisation of personal data.

Removal from the Digital Verification Services Register

45. The Secretary of State will have the power, under clause 52, to remove an organisation from the DVS Register. The effect of this would be that that organisation 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 54.

46. While this would not necessarily prevent the organisation from providing digital verification services, it may significantly affect business to the extent that the organisation relied on public authority information or the recognition of the trust mark. In this respect, and to this degree, inclusion on the register can be seen as akin to a licence, and thus a decision to remove an organisation from the register under clause 52 could amount to the determination of a civil right engaging Article 6 ECHR (see,

for example *Tre Traktörer Aktiebolag v. Sweden (1989)*).

47. 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 clause 52 satisfy fairness requirements. These include requirements for the Secretary of State to give notice stating reasons of her intention to remove an organisation from the register and the right for such an organisation to make representations (including, in some cases, the oral representations).

Digital Verification Services and data sharing by public authorities

48. Part 2 of the Bill provides for a power for a public authority to share personal data with a registered organisation for the purposes of providing identity and eligibility verification services where an individual has requested those services. The organisation 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 organisation 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.

49. The disclosure of personal data by a public authority under this power and the processing of that personal data by registered organisations 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.

50. 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 organisation, it demarcates the scope of that power. It provides that a public authority can only share information with an organisation that has been certified as meeting the technical requirements of the digital verification services trust framework including compliance with the DPA 2018 and the UK GDPR and has been registered by the Secretary of State. It also provides that a public authority can only share information where an individual makes a request to a registered organisation for the provision of identity or eligibility services. In practice this means the individual will create an online account with that organisation through which they will request the organisation verifies their identity or certain attributes about them against information held by a public authority which can be passed on to the relying party.

51. Public authorities will have to have due regard to a data sharing code of practice, to be laid before Parliament and 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 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 UK GDPR.

52. 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 *(Z v Finland).* Disclosure by public authorities is permitted, not mandated and must comply with data protection legislation. Individuals do not have to use digital identity verification and eligibility services and traditional methods of confirming identity such as passports remain an option for those who wish to use them. The requirements of the verification services trust framework and 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.

Customer data and business data (smart data)

53. Part 3 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.

54. The principal provisions of regulations made under Part 3 will be for a customer, or an authorised intermediary, to require a supplier of goods or services or digital content specified in those regulations, or a connected person, to provide the customer, or the intermediary, with data relating to that customer's transactions ("customer data": clause 62(1)) and contextual information relating to the goods, services or digital content supplied ("business data": clause 64(1)). "Ancillary" powers may require suppliers to produce, collect and/or retain data (clauses 62(2)(a) and 64(2)) and to rectify inaccurate customer data (clause 62(2)(b)). To allow customers to achieve tangible benefits from access to their data, the regulations may allow an intermediary to act on behalf of the customer in exercising rights that the customer has against the supplier (clause 62(3)): for instance, in a banking context that might include the intermediary accessing the customer's account to make a payment or negotiating an improved deal on the customer's behalf. There are also powers for accreditation of intermediaries, including an ability of a decision-maker to suspend or revoke it (clause 66), enforcement powers (clauses 67-69) which are considered in the context of Article 6, and powers to impose fees (clause 70) or a levy (clause 71) to cover costs.

55. 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.

56. The clauses are designed to build on the data portability right under Article 20 of the 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 follow 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.

57. Clauses 62(4) and 64(3) 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 (clauses 62(4) and 64(3)). Consultation and affirmative Parliamentary scrutiny 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 or which contain enforcement or revenue-raising provisions (clause 74(3) and (6)).

Article 8

58. Article 8 is potentially relevant to regulations under Part 3 as customer data is likely to be personal data and may therefore relate to an individual's private life.

59. The Department considers that regulations are fundamentally designed to improve the ability of customers, or intermediaries authorised by them, to access their data. As identified in the June 2019 public consultation Smart Data: Putting consumers in control of their data and enabling innovation,[2] the purpose of smart data schemes which are to be established by the regulations is to ensure that customers' data works for them and not against them. Furthermore, 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.

60. 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 of the UK

[2] https://www.gov.uk/government/consultations/smart-data-putting-consumers-in-control-of-their-data-and-enabling-innovation

GDPR.

61. 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.

62. Clause 73(1) provides powers to ensure that the processing of data does not breach obligations of confidence or other processing restrictions. Clause 73(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 of the UK GDPR and indeed clause 62(2)(b) provides powers for customers to request changes to customer data including rectification. Clause 73 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.

63. 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 74(1)). Furthermore, the statutory considerations to which the Secretary of State or the Treasury must have regard before making regulations (clauses 62(4) and 64(3)) and requirements of consultation (clause 74(6)) should also facilitate a proportionate approach in the regulations.

64. Finally, the regulations may contain provision requiring an enforcer to publish information relating to the exercise of decision-making or enforcement functions (clauses 66(7) and 67(9)). 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 DBT's "name and shame" publication scheme for breach of national minimum wage legislation.

Article 1 of Protocol 1

65. Some or all data held by the supplier, in particular business data may, as an asset of commercial value, be a "possession" (for instance, goodwill is a possession: *Van Marle v Netherlands* [1986] 8 EHRR 483; *Iatrides v Greece* [2000] 30 EHRR 97).

66. 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.

67. The clauses contain revenue raising powers to make provision for the payment of fees (clause 70) and for a levy (clause 71). The purpose of these powers is to ensure that smart data schemes are "self-funding" and revenue-neutral to the exchequer with enforcers and decision-makers 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. The Department considers that these clauses, and the provisions on fines and financial penalties (clauses 67(5) and (6) and 69), secure the payment of taxes or other contributions or penalties and are therefore permitted by the second paragraph of Article 1 of Protocol 1.

68. 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 the requirement of consultation.

Article 6

69. The enforcement provisions of regulations may include the issue and publication of compliance notices (clause 67(4)) and the imposition of fines and financial penalties (clauses 67(5) and (6) and 69) by an enforcer and revocation or suspension of the

approval of intermediaries who are allowed to act on behalf of the customer (clause 66(3)). Except for the possibility of provision of criminal offences for the provision of false or misleading information and other falsification (clause 67(5)), the enforcement regime is civil, and to be imposed administratively by enforcers, although the imposition of financial penalties (clause 67(6)) might in substance amount to a quasi-criminal charge (*Competition and Markets Authority v Flynn Pharma Ltd and another; Competition and Markets Authority v Pfizer Inc and another* [2022] UKSC 14 (SC)).

70. The Department again considers that the design of the powers, and constraints they impose, should ensure compatibility with Article 6. The regulations may make provisions about the rights of persons affected by the exercise of an enforcer's functions including provisions for reviews and appeals (clause 67(6)). However, the regulations must make such provisions where a decision-maker suspends or revokes the ability of an intermediary to receive data (clause 66(6).

71. The power of enforcers to impose financial penalties is subject to strict requirements as to its procedure including the opportunity to make representation and a requirement that the regulations contain provision for appeals to a court or tribunal (clause 69(3)).

72. Finally, all regulations containing any provisions relating to enforcement are subject to consultation and to affirmative Parliamentary scrutiny (clause 74(3)(d) and (6)).

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

Information standards for health and social care

Article 6

74. The imposition of specifications through information standards, the accreditation scheme, and the enforcement of the measure (via monitoring, compliance requests, financial penalties and a power for the Secretary of State, if he has reasonable grounds to suspect that an information technology provider or processor is not complying with an information standard, to publish a statement to that effect ("public censure provision") could engage Article 6 as they could involve a determination of

the civil rights of information technology providers and processors to carry on the commercial activity of supply information technology, information technology services or IT processing services (services consisting of processing information using IT), to the health and social care sector (insofar as providers and suppliers are not themselves public authorities, for example in-house providers of public authorities).

75. Article 6 provides that everyone, in the determination of his or her civil rights and obligations or of any criminal charge against him, is entitled to a fair and public hearing. The Department considers that the power to publish binding information standards under Part 4 is properly characterised as an exercise of administrative discretion, and therefore that it is the type of decision which is 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.

76. The powers are thus capable of being exercised compatibly with the ECHR, including 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 clauses would trigger provisions about appeals to independent bodies (the First-Tier tribunal). In summary, the Department is of the opinion that the imposition of the information standards is compatible with Article 6 of the ECHR, 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

77. The Department considers that the imposition of information standards, the accreditation scheme, and the enforcement of the measure (via monitoring, compliance requests, financial penalties and the public censure provision) could engage Article 1 of Protocol 1 as they could impact on the ability of information technology providers to carry on private commercial activities for profit.

78. 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 clauses 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 as well as on providers of IT processing services.

79. The standards would be limited to those which are necessary to achieve these aims and the powers are capable of being exercised compatibility 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, the clauses 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.

The Information Commission: Article 1 of Protocol 1

80. The Bill abolishes the office of the Information Commissioner (ICO) (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 (IC) being discharged by the board of the new body, the Information Commission, rather than being vested in and formally discharged by the IC, 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.

81. The Bill provides (via transitional provision in draft Schedule 13) that the IC is transitioned into the role of chair of the board of the new body, for a term that expires

at the time that the IC 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 A1P1: there's a strong rationale for the changes made in the Bill and, on the basis that the IC 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 IC's tenure and remuneration package will be protected.

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

March 2023