DATA PROTECTION AND DIGITAL INFORMATION BILL

Memorandum from the Department for Science, Innovation and Technology to the Delegated Powers and Regulatory Reform Committee

A. INTRODUCTION

1. This memorandum has been prepared for the Delegated Powers and Regulatory Reform Committee by the Department for Science, Innovation and Technology ("DSIT") to assist with its scrutiny of the Data Protection and Digital Information Bill ("the Bill").

2. The Bill was introduced in the House of Commons on 8 March 2023 and carried over into the 4th Parliamentary Session. This revised memorandum reflects the changes made to the Bill at Committee Stage in the House of Commons.

3. This memorandum identifies the provisions of the Bill that confer powers to make delegated legislation. It explains in each case why the power has been taken and explains the nature of, and the reason for, the procedure selected.

B. PURPOSE AND EFFECT OF THE BILL

4. The Bill makes provision for a variety of measures relating to personal data and other information, including digital information.

5. Part 1 of the Bill makes various changes to the UK's data protection framework, as set out in the UK GDPR[1] and the Data Protection Act 2018 ("DPA 2018"), which regulates the processing of personal data. The existing data protection legislation provides for data protection principles, the grounds on which personal data may be processed, particular restrictions on processing sensitive personal data, rights of data subjects, obligations of data controllers and processors, and enforcement matters. The legislation provides for a regulator, the Information Commissioner, and sets out matters relating to its governance. The existing legislative framework comprises three data protection regimes:

    a. for general processing of personal data ("the general processing regime");

    b. for processing by "competent authorities" (e.g. the police) for law enforcement purposes ("the law enforcement regime"); and

    c. for processing by the intelligence services ("the intelligence services regime").

6. Part 1 makes changes to each of these regimes.

7. Changes to the general processing regime include changes in relation to processing for research purposes, the lawful grounds for processing personal data, data subject access rights, automated decision-making ("ADM"), compliance obligations and international data transfers.

8. Changes to the law enforcement regime include changes in relation to conditions to consent for processing, data subject requests, exemptions for legal professional privilege and national security, automated decision-making, compliance obligations, codes of conduct, and international data transfers.

[1] Retained direct principal EU legislation, as defined in the European Union (Withdrawal) Act 2018

9. Changes to the intelligence services regime include changes in relation to data subject requests, automated decision-making, and provision enabling processing by "competent authorities" to take place under the intelligence services regime, instead of the law enforcement regime, in certain circumstances.

10. This part of the Bill also provides the Information Commissioner with additional enforcement powers.

11. Part 2 of the Bill establishes a regulatory framework for the provision of digital verification services in the UK and enables public authorities to disclose information relating to an individual to trusted organisations providing such verification services.

12. Part 3 of the Bill provides powers to enable the establishment of "smart data" schemes. These schemes will enable the secure sharing of customer data, upon the customer's request, with authorised third-party providers, which can use the customer's data to provide services for the customer or business as well as sharing or publication of contextual business data.

13. Part 4 of the Bill makes changes to the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("the PEC Regulations"). These regulations include special rules which supplement the data protection legislation in relation to the processing of personal data through the use of cookies and for direct marketing purposes, including nuisance calls. The Bill makes some changes to these provisions, and also applies the DPA 2018 enforcement regime to the regulations, which are currently subject to the enforcement regime under the Data Protection Act 1998.

14. Part 4 also extends an existing power in the Digital Economy Act 2017, which allows for data sharing that benefits households and individuals, to additionally allow data sharing to deliver public services that benefit businesses and other forms of undertaking.

15. Part 4 also provides a power for the Secretary of State to make regulations in relation to the implementation of international data sharing agreements.

16. Part 4 also removes the requirement for paper registers of births and deaths and enables them to be registered electronically.

17. Schedule 12 concerns standards relating to the processing of information ("information standards") in relation to the health and adult social care sector enabling such information standards to be applied to providers of IT and related services. It does this by making clear that information standards published under section 250 of the Health and Social Care Act 2012 include standards relating to IT or IT services, and extending the persons to whom information standards may apply to persons who make available IT, IT services or information processing services using IT, in connection with the provision in, or in relation to, England, of health or adult social care.

18. Part 5 and Schedule 13 establishes a statutory corporation, with a new governance structure, to replace the office of the Information Commissioner.

19. Part 5 also changes the oversight framework for the police use of biometrics and police and local authority use of surveillance cameras, abolishing the offices of the Commissioner for the Retention and Use of Biometric Material and the Surveillance Camera Commissioner and transferring some functions to the Investigatory Powers Commissioner. It also updates the scope of the police National DNA Database Board and provides the Secretary of State with a power to amend the scope of the Board.

20. To support its policy objectives, the Bill includes a number of delegated powers. Many of these build on or have precedents in existing powers and frameworks in current legislation, as described in further detail in Section C. In the majority of cases regulation-making powers are subject to consultation requirements. In general terms, powers in relation to data

protection and privacy laws and for information standards for health and adult social care build on existing frameworks. Powers in Part 2 of the Bill support the creation of a new framework and where appropriate precedents for these have been identified. Powers in Part 3 of the Bill replace an existing statutory framework with a new, enhanced one.

21. This is an updated version of a Bill previously introduced in July 2022 (the Data Protection and Digital Information Bill). There are two additional powers compared to the previous Bill, which are in new Article 22D(1) UK GDPR and new s50(D)(1) DPA 2018, both added by clause 12 of the Bill.

C. DELEGATED POWERS

22. The Bill includes the following delegated powers.

Clause 5(4): Power to amend new lawful ground for processing

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

23. Clause 5 amends Article 6(1) of the UK GDPR to add a new lawful ground for processing personal data (new Article 6(1)(ea): processing necessary for the purposes of a recognised legitimate interest). It also inserts a new Annex 1 into the UK GDPR to set out the detailed conditions relating to the new lawful ground. These include important public interest grounds such as safeguarding vulnerable adults and children, safeguarding national security, public security and defence or where a public authority requests information that may include personal data. Under current law non-public authority data controllers would need to conduct a balancing of interests test to determine whether personal data should be processed for these purposes (Article 6(1)(f) UK GDPR). Some responses to the consultation, *Data: A New Direction*, indicated that the need to carry out a balancing exercise when relying on the legitimate interests lawful ground (Article 6(1)(f)) can cause risk aversion. If a data controller is not sure whether its interests outweigh the rights of the individual, it might decide to delay or stop the processing data due to worries about liability. The government considers that these areas are sufficiently important to dispense with the need for the balancing of interests test and that the burden should not be on data controllers in these circumstances. New Article 6(6) UK GDPR, inserted by clause 5(4), introduces a regulation making power to amend Annex 1 by adding to or varying the conditions or omitting conditions added by regulations.

Justification for taking the power

24. The government is proceeding with the limited list of conditions set out in new Annex 1 on the basis that this is a departure from long-standing and well-understood lawful grounds for processing and will need to assess the extent to which they are relied on. However, the government is concerned that difficulties applying the balancing test in Article 6 (1)(f) for other processing activities may come to light in the future, interfering with important processing, particularly in light of wider changes made to the lawful ground for processing in the Bill. The grounds might alternatively need to be varied, for example to add additional safeguards if they were being relied on inappropriately by data controllers, or new grounds added by Regulations might need to be omitted for similar reasons. The ability for the government to act swiftly in these circumstances justifies the need for a regulation making power in order to account for these situations.

25. The power allows direct amendment of Annex 1 in order to ensure legislative coherence and clarity for the reader. Data controllers and data subjects are used to being able to consult Article 6(1) UK GDPR to identify lawful grounds and will now need to consult Annex 1 also. The government would like to keep these additions to the lawful processing grounds in one place given their fundamental importance to the data protection framework. This approach of making direct amendments to the DPA 2018 is consistent with existing regulation making powers in the DPA 2018 that permit exemptions from important principles and rights (eg. section 16(1)(b) - powers to exempt from data subject rights and section 10(6) power to add, vary or omit conditions added by regulations in relation to the processing of sensitive data). There are limitations on the power: no provisions that were added to Annex 1 by primary legislation can be omitted. Also, the Secretary of State must take into account the interests and fundamental rights and freedoms of data subjects and the need to provide special protection of children before making any regulations. This requirement reflects the factors that are required to be taken into account under the existing balancing test in Article 6(1)(f) UK GDPR.

26. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see new Article 91A UK GDPR added by clause 46 of this Bill).

Justification for the procedure

27. By virtue of new Article 6(8) UK GDPR (as inserted by clause 5(4)), the regulations are subject to the affirmative procedure. This level of scrutiny is considered appropriate given that the regulations permit changes to fundamental lawful processing grounds. The affirmative procedure is also appropriate given that this power will permit direct amendments to the UK GDPR (retained direct principal EU legislation) so that new cases can be added directly to Annex 1. Given that the effect of clause 5 is to introduce new lawful grounds that are exempt from the balancing of interests test, the procedure is consistent with existing regulation making powers in DPA 2018 that permit exemptions from important principles and rights (eg. section 16(1)(b) - powers to exempt from data subject rights) - and section 10(6) - power to add, vary or omit conditions added by regulations in relation to the processing of sensitive data).

Clause 6(5): Power to amend conditions in which processing is treated as compatible with the original purpose

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

28. Clause 6(6) inserts new Annex 2 into the UK GDPR. Annex 2 sets out a limited set of circumstances in which processing of personal data for a different purpose is treated as compatible with the original purpose without a specific law being required. The context for these provisions is that the existing law as set out in the UK GDPR (carried over on EU exit from the EU GDPR) is confusing. The main provision in the text (Article 6(4) UK GDPR) is poorly drafted, and is supported by a recital (with non-legislative effect)- recital 50- which provides more detail but is also difficult to decipher. As such, controllers and data subjects have had difficulty accessing these important rules, which relate to a fundamental principle in the UK GDPR that processing in a manner incompatible with the original purpose is not permitted. New Article 8A(5) contains a regulation making power to amend Annex 2 by adding to or varying the provisions in the Annex or omitting provisions added by regulations made under Article 8A(5). The power can only be exercised where the Secretary of State considers

that processing in these cases is necessary to safeguard an objective listed in Article 23(1)(c) to (j) of the UK GDPR. New Article 8A(7) sets out some specific provisions that may be made under the power.

Justification for taking the power

29. The power is needed because new Article 8A is clarifying the rules on purpose limitation to make them easier for data controllers and data subjects to understand them. The rules affect data controllers across all sectors of the UK. There is a risk that in clarifying those rules for the first time, certain important public interest processing activities are inadvertently affected, given that the current rules allow for a degree of ambiguity in interpretation. Controllers may only realise that these problems arise when they come to apply the new rules to processing activities. It is important that the government is able to deal with any such situations swiftly and on a case by case basis in case the codification of these rules leads to the impediment of important processing for an important objective of public interest, for example. It is also important that where new exemptions are added but evidence arises that these are being relied on inappropriately, these are able to be removed or varied.

30. The power allows direct amendments of Annex 2 in order to ensure legislative coherence and clarity for the reader. Data controllers and data subjects will need to consult Annex 2 and provisions in the main body of the UK GDPR to understand the framework for processing personal data for a different purpose. The key aim of clause 6 is to provide clarity for data subjects and data controllers around an important data processing principle that has previously been lacking. Having a coherent and complete set of rules around processing for a different purpose in new Article 8A and Annex 2 will give controllers more confidence about using personal data correctly and data subjects a better understanding of their rights. This approach of making direct amendments to DPA 2018 is consistent with existing regulation making powers in DPA 2018 that permit exemptions from important principles and rights (eg. section 16(1)(b) - powers to exempt from data subject rights - and section 10(6) - power to add, vary or omit conditions added by regulations in relation to the processing of sensitive data). By way of limitation on the power, it does not permit conditions that were added by primary legislation to be omitted.

31. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see new Article 91A UK GDPR added by clause 46 of this Bill).

Justification for the procedure

32. By virtue of new Article 8A(8), as inserted by this clause, the regulations are subject to the affirmative procedure. This level of scrutiny is considered appropriate given that the new cases that can be added by regulations amount to exemptions from one of the key data protection principles (the purpose limitation principle in Article 5(1)(b) UK GDPR). The affirmative procedure is also appropriate given that this power will permit direct amendments to the UK GDPR (retained direct principal EU legislation) so that new cases can be added directly to Annex 2. The procedure is consistent with existing regulation making powers in DPA 2018 that permit exemptions from important principles and rights (eg. section 16(1)(b)- powers to exempt from data subject rights) and section 10(6)- power to add, vary or omit conditions added by regulations in relation to the processing of sensitive data).

Clause 7(6)(f): Power to require controllers to produce guidance about fees

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Negative procedure

Context and Purpose

33. This clause amends section 53 DPA 2018 and changes the legal test set out for controllers to charge a fee or refuse to comply with a Subject Access Request (SAR). The test is amended from "manifestly unfounded or excessive" to "vexatious or excessive". The provision will allow controllers to charge a reasonable fee for dealing with a SAR (or to refuse to comply) when the request is deemed "vexatious or excessive". This clause amends existing regulation making powers already conferred to the Secretary of State by section 53. The Secretary of State has the power to specify by regulations limits on the fees that a controller may charge under section 53. The amendment will also allow the Secretary of State to:

    a. Require controllers to produce and publish guidance about the fees that they charge in reliance of section 53 DPA 2018 as amended, and

    b. Specify what this guidance must include.

Justification for taking the power

34. The Secretary of State has an existing regulation making power in section 53(4) DPA 2018 to specify limits on the fees that a controller may charge under section 53. The new power in subsection 4A of section 53 of the DPA is needed so that the Secretary of State may also make regulations requiring controllers to produce and publish guidance about the fees they can charge.The purpose of this new power is to ensure that there is consistency and to reduce fragmentation across the Part 2 and Part 3 regimes. An equivalent regulation-making power that already exists in connection with general processing subject to the UK GDPR (see section 12(2) of the DPA).

35. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see section 182 DPA 2018).

Justification for the procedure

36. The existing regulation making power under section 53(4) DPA 2018 is subject to the negative resolution procedure and the additional power in section 53(4A), will be subject to the same procedure. The negative procedure remains appropriate as it affords the appropriate level of parliamentary scrutiny for the existing power in s. 53(4) and for the new power to require controllers to produce and publish guidance about fees that they charge . The power to make regulations pursuant to section 12(2) DPA 2018 in respect of controllers processing under the UK GDPR (which this provision is reading across to Part 3), is also subject to negative procedure

Clause 12 re: automated decision-making for general/commercial processing

Clause 12: Powers to amend the application of Article 22A (new Article 22D(1) and Article 22D (2))

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

37. Article 22 of the UK GDPR sets out the conditions under which solely automated decisions, including profiling, that produce legal or similarly significant effects on data subjects may be carried out ("qualifying ADM"). Existing Article 22 restricts such activity to three conditions: (i) where necessary for entering into, or the performance of, a contract between a controller and a data subject, Article 6(1)(b) UK GDPR; (ii) where such activity is required or authorised by law (which includes circumstances where the processing is necessary to comply with legal obligation, Article 6(1)(c) UK GDPR or to perform a public task, Article 6(1)(e) UK GDPR); or (iii) where a data subject has provided explicit consent, Article 6(1)(a) UK GDPR.

38. Clause 12 replaces Article 22 of the UK GDPR with new Articles 22A-22D which expand the scope of existing Article 22 to all lawful bases for processing personal data to permit processing necessary to protect vital interests, Article 6(1)(d) UK GDPR, and necessary for the purpose of legitimate interests, Article 6(1)(f) UK GDPR.

39. New Article 22A(1)(a) introduces a definition of a decision based on solely automated processing as one that involves no meaningful human involvement. New Article 22A(1)(b)(i) and (ii) set out the meaning of a significant decision as one that produces legal or similarly significant effects on a data subject. New Article 22B(1)-(3) sets out the restrictions on qualifying ADM in respect to sensitive personal data. New Article 22B(4) prohibits a reliance on new Article 6(1)(ea) for the purposes of carrying out qualifying ADM. New Article 22C sets out the safeguards that must be applied when undertaking qualifying ADM. The government requires regulation-making powers to amend new Article 22A(1).

Justification for taking the power

40. The government requires delegated powers which will allow a dynamic response to the growing evidence base that will emerge from the increased adoption of evolving technologies using solely automated decision-making. The powers will provide clarity to data subjects and controllers as to whether an activity falls within scope of new Article 22A. There are two powers which are required:

    a. The power in Article 22D(1) will enable the Secretary of State to bring in regulations to provide, for the purposes of Article 22A(1)(a), what is, or is not, to be taken to be meaningful human involvement in particular cases. Given the range of use cases that fall within the scope of Article 22A, and the fast-moving pace of innovation and uptake of technology using automated decision-making, it would not be feasible to address the range of specific cases that require clarity, within the timescales needed in practice, in primary legislation. For example, the application of this power is likely to relate to some significant decisions that are taken on the basis of profiling as defined in Article 4(4) UK GDPR, an automated process which, in some cases, can play a heavy role in determining the outcome reached for a data subject. Since profiling can be used in a diverse set of ways and can be relied on to different degrees in different contexts, a delegated power may be exercised to provide legal certainty, if and when, a growing evidence base suggests that certain applications should or should not be regarded as having meaningful involvement. This is necessary to ensure the circumstances in which the prohibitions in Article 22B and applicable safeguards in new Article 22C UK GDPR apply are clear. In contrast a regulation-making power that does not permit the amendment of the UK GDPR would lead to legislative discontinuity given the necessary information is not all in one place. Article 22D(3) enables regulations made under new Article 22D(1) to directly amend Article 22A(1)(a).

b. The power in new Article 22D(2) serves a similar purpose, ensuring Article 22A(1)(b)(ii), can be amended as necessary to keep pace with the adoption of technologies using solely automated decision-making. The regulation-making power will enable the government to describe decisions that are and are not to be taken as having a "similarly significant effect" for the purposes of Article 22A(1)(b)(ii). This is necessary to ensure the circumstances in which the specific safeguards should apply are clear, and can be updated in line with societal expectations of what constitutes a significant effect in a privacy context. Article 22D(3) enables regulations made under new Article 22D(2) to directly amend Article 22A(1)(b)(ii). The power in Article 22D(2) will ensure legislative coherence and clarity for the reader and user.

41. Before making regulations under these powers the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see new Article 91A UK GDPR added by clause 46 of this Bill).

Justification for the procedure

42. Both of the powers in Article 22D(1) and Article 22D(2) are subject to the affirmative procedure. This level of scrutiny is considered appropriate given that the regulations will be capable of making changes to retained direct principal EU legislation.

Clause 12: Power to amend safeguards for automated decision-making (New Article 22 D(4))

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

43. There are existing safeguards in place to protect the rights and freedoms of data subjects where a significant decision has taken place based solely on automated processing. These are currently contained in Article 22(3)-(3A) of the UK GDPR and are supplemented by section 14 DPA 2018. Under the safeguards in Article 22(3), controllers are required to put in place suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. Under the safeguards in section 14(4) DPA 2018 the controller must notify the data subject that a decision has been taken based solely on automated processing and within a month of notification the data subject can ask the controller to (i) reconsider the decision, or (ii) take a new decision that is not based solely on automated processing. The controller must then comply with the request pursuant to section 14(5) DPA 2018.

44. There is a significant amount of overlap between the existing safeguards which need to be met by controllers (and processors acting on their behalf) when qualifying ADM is undertaken that are set out in Article 22(3) (ie. where ADM is necessary for the performance of a contract or based on the data subject's explicit consent) and those set out in section 14 DPA 2018 which implement the safeguards provided for in Article 22(2)(b) (ie. where ADM is required or authorised by domestic law).

45. Clause 12 replaces the existing safeguards in Article 22 UK GDPR and section 14 DPA 2018 with new Article 22C, which simplifies and consolidates these safeguards for qualifying ADM. These safeguards include (i) the right to be provided with information with respect to significant decisions taken using solely automated processing; (ii) to make representations about such decisions; (iii) to obtain human intervention on the part of the controller in relation to such decisions and (iv) to contest such decisions.

46. There is an existing power in section 14(7) DPA 2018 for the Secretary of State to add or amend current safeguards, which may be exercised to amend section 14 itself. New Article 22D(4) provides a similar power for the Secretary of State to make further provisions about the safeguards required in new Article 22C(1), including provisions about what is, or is not, to be taken to satisfy a requirement under Article 22C(1) or Article 22C(2) directly; New Article 22D(4) creates a new regulation making power for the Secretary of State to (i) add new free-standing safeguards (ii) add or vary safeguards listed in Article 22C in regulations and (iii) omit provisions added by regulations made under 22D(4).

Justification for taking the power

47. The government believes a new power is necessary to ensure that the safeguards remain appropriate and effective, in light of the fast-moving advances and adoption of technologies relevant to automated decision-making. This will ensure data subjects are afforded sufficient protections against risks to their rights and freedoms being infringed when their personal data is processed for qualifying ADM purposes. New Article 22D(5) enables regulations to add, or vary safeguards and/or remove safeguards added by regulations, but importantly it does not include a power to remove safeguards provided in new Article 22C and therefore cannot be exercised to weaken the protections Article 22 affords to data subjects.

48. This power may be exercised to ensure the safeguards remain fit for purpose. This is in light of the rapid advancement and adoption of technologies related to automated decision-making that may inform when meaningful involvement can be said to have taken place, as well as changing societal expectations of what constitutes a significant decision in a privacy context.

49. The power is similar to the existing power under section 14(7) DPA 2018 to add or amend safeguards, but cannot be used to omit safeguards other than those which have been added through the exercise of the new power.

50. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see new Article 91A UK GDPR added by clause 46 of this Bill).

Justification for the procedure

51. New Article 22D(6) provides that regulations made under Article 22D(3) are subject to the affirmative procedure. This is considered appropriate given the exercise of the power could alter what safeguards are in place to protect the rights and freedoms of data subjects. The affirmative procedure is also appropriate given that this power will permit direct amendments to retained direct principal EU legislation so that new safeguards can be added directly to Article 22C. The existing power under section 14(7) DPA 2018 is subject to the affirmative procedure.

Clause 12: Powers for automated decision-making in the law enforcement context under Part 3 DPA 2018

Clause 12: Powers to amend the application of new section 50A (new sections 50D(1) and 50D(2))

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

52. These changes to the Part 3 regime mirror the equivalent Clause 12 amendments to the UK GDPR set out above, and will therefore apply to automated decision-making in the law enforcement context.

Context and Purpose

53. Sections 49 and 50 DPA 2018 provide limitations and safeguards on solely automated decisions under Part 3 of the DPA 2018 (applicable to law enforcement processing), that produce adverse legal or other significant effects on data subjects. Such activity is only permitted where it is required or authorised by law.

54. Clause 12 repeals sections 49 and 50 DPA 2018, replacing them with new sections 50A-D. These new sections align the approach in Part 3 of the DPA with that being provided for in the new Articles 22A-D in the UK GDPR, reflecting the broader aim to ensure consistency across the data protection regimes where possible. New section 50A introduces a definition of 'a decision based on solely automated processing', as one that involves no meaningful human intervention. Sections 50A(1)(b)(i) and (ii) set out the meaning of a significant decision as one that produces adverse legal or similarly adverse significant effects on a data subject. New section 50B provides restrictions on automated decision-making using sensitive personal data and new section 50C details the safeguards that must be applied when undertaking automated decision making. New section 50D(1) and 50(2) mirrors the powers of the Secretary of State, set out under Article 22D(1) and 22D(2) to make further provisions about automated decision-making relating to the scope of section 50A(1).

Justification for taking the power

55. These changes to the Part 3 regime mirror the equivalent Clause 12 amendments to the UK GDPR set out above. In order to be consistent, they therefore adopt the same approach to powers as those provisions thereby bringing clarity to both controllers and data subjects. The justification is therefore the same as already detailed above for the equivalent UK GDPR reforms. The powers will also enable Part 3 controllers, as with their UK GDPR counterparts, to take a dynamic response to the growing evidence base that will emerge from the increased adoption of evolving technologies using solely automated decision-making. As with the UK GDPR, there are two powers which are required:

    a. The power in subsection 50D(1) will enable the Secretary of State to bring in regulations to provide for the purposes of section 50A(1)(a); i.e., to specify what is, or is not, to be taken to be meaningful human involvement. Subsection 50D(3) enables regulations made under new subsection 50D(1) to amend section 50A(1)(a) directly. 50D(1) is therefore a Henry VIII power that will provide clarity for controllers. Given the range of use cases that fall within the scope of Section 50A, and the fast-moving pace of innovation and uptake of technology using automated decision-making, it would not be feasible to

address the range of specific cases that require clarity, within the timescales needed in practice, in primary legislation. For example the application of this power is likely to relate to some significant decisions that are taken on the basis of profiling as defined in Article 4(4) UK GDPR, an automated process which, in some cases, can play a heavy role in determining the outcome reached for a data subject. Since profiling can be used in a diverse set of ways and can be relied on to different degrees in different contexts, a delegated power may be exercised to provide legal certainty, if and when, a growing evidence base suggests that certain applications should or should not be regarded as having meaningful involvement. This is necessary to ensure the circumstances in which the prohibitions in section 50B and applicable safeguards in new section 50C apply are clear. In contrast a regulation-making power that does not permit the amendment of primary legislation would lead to legislative discontinuity given the necessary information is not all in one place. This Henry VIII power will enable both rapid agile changes providing legal certainty, as well as importantly ensuring legislative coherence, clarity and simplicity for the reader. Para. 80-82 of the Delegated Powers and Regulatory Reform Committee, 12th Report of Session 2021–22[2]) recognises that there are times when it is appropriate to use a Henry VIII power. We therefore consider the powers within Clause 12 (in the UK GDPR regime and Part 3 DPA 2018) fall within these circumstances.

b.The power in subsection 50D(2), which will enable regulations to clarify the scope of new section 50A(1)(b)(ii) i.e. what is or is not to be taken to have a "similarly significant adverse effect" on the data subject. Subsection 50D(3) enables regulations made under new subsection 50D(2) to amend section 50A(1)(b)(ii)) directly. The power in subsection 50D(2) is therefore a Henry VIII which will provide consistency across the legislation and clarity for controllers and will ensure it can be amended as necessary to keep pace with the adoption of technologies using solely automated decision-making. The regulation- making power will enable the government to describe decisions that are and are not to be taken as having a "similarly significant effect." This is necessary to ensure the circumstances in which the specific safeguards should apply are clear, and can be updated in line with societal expectations of what constitutes a significant effect in a privacy context.

56. Before making regulations under these powers the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see section 182 DPA 2018).

Justification for the procedure

57. The powers in subsection 50D(1) and 50D(2) are subject to the affirmative procedure. This level of scrutiny is considered appropriate given that the regulations will permit the Secretary of State to amend the scope of section 50A.

Clause 12: Power to change safeguards for automated decision-making under Part 3 DPA 2018 (New subsection 50D(4))

2 Democracy Denied? The urgent need to rebalance power between Parliament and the Executive, 12th Report of Session 2021–22, published 24 November 2021 https://committees.parliament.uk/publications/7960/documents/82286/default/

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

58. There are existing safeguards in place to protect the rights of data subjects where a qualifying significant decision has taken place based solely on automated processing. These are currently provided for in section 50 of the DPA 2018 and it includes the right for the data subject to ask the controller to review any such decision, with the controller taking a new decision that is not based solely on automated processing.

59. The new section 50C replaces these existing safeguards in section 50, with a similar set of safeguards, but mirroring the drafting approach and reforms being made to the UK GDPR (with the new Article 22C) to ensure greater consistency between the regimes. This includes (i) the right to be provided with information with respect to significant decisions taken using solely automated processing; (ii) to make representations about such decisions; (iii) to obtain human intervention on the part of the controller in relation to such decisions and (iv) to contest such decisions.

60. Subsection 50D(4) creates a new regulation making power for the Secretary of State to (i) add new free-standing safeguards (ii) add or vary safeguards listed in 50C in regulations (iii) and omit provisions added by regulations made under 50D(4).

Justification for taking the power

61. As already detailed above for the equivalent UK GDPR reforms, the government believes a new power (in this case a Henry VIII power) is necessary to ensure that the safeguards for significant decisions made using automated decision-making under Part 3 are aligned with those under UK GDPR thereby bringing clarity to both controllers and data subjects. The powers will also enable Part 3 controllers, as with their UK GDPR counterparts, to ensure that they remain fit for purpose as the technology evolves. This will ensure there are sufficient safeguards in place to protect data subjects against risks to their rights and freedoms in light of rapid advancement in technology when personal data is being processed for qualifying ADM purposes. This power will enable regulations to add or vary safeguards, remove safeguards added by regulation, but it will not allow the Secretary of State to remove the safeguards provided for in section 50C.

62. The Secretary of State already has a power under section 50(4) enabled by section 50(5) of the DPA 2018 to add or amend safeguards for significant decisions based solely on automated processing.

63. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see section 182 DPA 2018).

Justification for the procedure

64. The power in new subsection 50D(4) is subject to the affirmative procedure. Given that the power will permit the Secretary of State to directly amend subsection 50C(2) of the Act to vary the current safeguards (i.e. it is a Henry VIII power), this is considered appropriate given

the exercise of the power could alter what safeguards are in place to protect the rights and freedoms of data subjects.

65. The affirmative procedure is also appropriate given that this power will permit direct amendments to primary legislation so that new safeguards can be added directly to clause 50C. The existing power under section 50(4) of the DPA 2018 is subject to the affirmative procedure.

Clause 24(2): Power to amend safeguards for processing for research etc purposes

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

66. There are existing safeguards in place to protect the rights and freedoms of data subjects when their data is being processed for research purposes. This includes processing for scientific research, historic research, archiving in the public interest and processing for statistical purposes. These are currently contained in Article 89(1) of the UK GDPR as supplemented by section 19 DPA 2018. Under these safeguards, organisations are required to put in place technical and organisational measures, such as pseudonymisation, to protect the rights of data subjects when they are processing for research purposes. There is also a prohibition on processing for research purposes if processed in such a way that causes substantial damage or distress to the data subject. Processing that supports measures or decisions with respect to a particular individual unless the processing is for approved medical research as set out in section 19(4) DPA 2018 is also prohibited. There is an existing power in section 19(5) DPA 2018 to allow the Secretary of State to change the meaning of approved medical research by regulations.

67. Clause 24(2) will move and combine the existing safeguards in section 19 DPA 2018 and Article 89 UK GDPR for research, archiving and statistical purposes (referred to as RAS purposes) into a new Chapter 8A of the UK GDPR for greater clarity. Article 84B will set out what these safeguards are and Article 84C will make further provision as to when these requirements are met. This clause also creates a new power in Article 84D for the Secretary of State to make further provision as to when the requirement for appropriate safeguards is met under Article 84B. This power will allow the Secretary of State to add, vary or omit parts of Article 84C. The purpose of the power is to ensure that safeguards for RAS purposes are kept up to date as technology changes. While this power is a new power for the purposes of the new clause, it replicates and adds to the existing powers contained in s 19(5) which is to be omitted by the new clause.

Justification for taking the power

68. The government believes a new power is necessary to ensure there are sufficient safeguards in place to protect data subjects against risks to their rights and freedoms in light of rapid advancement in technology when their data is being processed for RAS purposes. This power will not allow the Secretary of State to omit existing safeguards in paragraphs 2-4 of the new Article 84C and will be limited to adding or varying these safeguards. The Secretary of State will also be able to amend the definition of “approved medical research” under this power by adding, varying or omitting paragraph 5 of Article 84C. This replaces the existing power in section 19(5) DPA 2018. This is considered necessary to ensure the definition of “approved medical research” is kept up to date to provide sufficient protections for data subjects when their personal data is being processed for RAS purposes.

69. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see new Article 91A UK GDPR added by clause 44 of this Bill).

Justification for the procedure

70. Regulations under new Article 84D will be subject to the affirmative procedure. This is considered appropriate given the exercise of the power could alter what safeguards are in place to protect the rights and freedoms of data subjects. The affirmative procedure is also appropriate given that this power will permit direct amendments to the UK GDPR (retained direct principal EU legislation) so that new safeguards can be added directly to Article 84C.

Clause 27(2): Power to specify which competent authorities may be issued with designation notices for joint processing with the intelligence services

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

71. This clause will enable specified qualifying competent authorities to process data under Part 4 of the DPA 2018 (the regime currently only applicable to the intelligence services) in limited circumstances. 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 competent authorities and intelligence services, which is judged to have significant operational benefits, enabling closer working in efforts to detect and combat national security threats.

72. The Secretary of State will have the power to issue designation notices, specifying that joint processing between the intelligence services and specified qualifying competent authorities, can be governed by Part 4 of the DPA 2018. Competent authorities are defined in section 30 of the DPA 2018, with a list of names authorities provided at Schedule 7 to the DPA 2018 (including the police, national crime agency etc.). The Secretary of State will have the power to make regulations which specify or describe which of these competent authorities should be treated as "qualifying competent authorities". This means notices cannot be issued to a competent authority listed in Schedule 7, unless specified in regulations made by the Secretary of State.

Justification for taking the power

73. This power is needed to ensure that the Secretary of State can specify which competent authorities can apply for and be subject to a designation notice. Competent Authorities are defined by s.30 DPA 2018 and are listed in Schedule 7, however it is recognised that it is unlikely to be necessary for notices to be issued to some of the competent authorities listed in Schedule 7, so it was important to have the ability to restrict the new notice provisions to a more limited range of "qualifying competent authorities". Given the exceptional effect of a designation notice it is essential that it can and should only be possible for such notices to apply where it is proportionate and necessary to do so. Listing qualifying competent authorities in the DPA 2018 itself was considered, but ultimately such an approach was rejected as tending to be overinclusive. It is more appropriate to consider on a case by case basis (as and when the need arises) whether a particular competent authority should be capable of being subject to a notice based on up-to-date information, rather than attempting to pre-empt such considerations by a wider general listing of such bodies on the face of the legislation. It is also recognised that the list at Schedule 7 to DPA 2018 could be subject to

further change, so creating a restrictive list of qualifying competent authorities at this stage would be duplicative and may mean it becomes out of date. The focused and specific regulation-making power ensures that the Secretary of State can more proportionately respond and keep under regular review which competent authorities should be regarded as qualifying.

74. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see section 182 DPA 2018).

Justification for the procedure

75. Regulations designating competent authorities as "qualifying competent authorities" will be subject to the affirmative procedure and require approval by both Houses of Parliament. It is considered that given the Secretary of State can issue designation notices to those competent authorities specified in such regulations, this procedure provides an appropriate level of Parliamentary scrutiny.

Clause 30(2): Power to designate a statement of strategic priorities

Power conferred on: Secretary of State

Power exercised by: Statement of Strategic Priorities

Parliamentary Procedure: Statement laid before Parliament and may not be designated if within the 40 day period after laying either House of Parliament resolves not to approve it.

Context and Purpose

76. This clause inserts new sections 120E to 120H into the DPA 2018 which provide a power for the Secretary of State to designate a statement setting out the government's strategic priorities relating to data protection (a statement of strategic priorities). The statement must be laid before Parliament and may not be designated if within the 40 day period after laying either House of Parliament resolves not to approve it (see new section 120G(2)). The Information Commissioner must have regard to a designated statement of strategic priorities when carrying out functions under the data protection legislation (excluding carrying out functions in relation to a particular person, case or investigation). The Information Commissioner must also publish an explanation of how the Commissioner will have regard to the designated statement of strategic priorities when carrying out these functions (new section 120F(3) and include a review of this in the Commissioner's annual report to Parliament (clause 30(3)).

77. The purpose of the statement of strategic priorities is to enable the government to set out its domestic and international data protection policies in a transparent way and to provide the Information Commissioner with useful context when carrying out its functions related to data protection. The government is committed to ensuring the Information Commissioner's continued independence, therefore, whilst the Commissioner will be required to have regard to the statement, and publish a response on it, the Commissioner will not be legally bound to act in accordance with it or to take it into consideration when making decisions on individual cases.

Justification for taking the power

78. It would not be appropriate to set out the government's strategic priorities relating to data protection in primary legislation because the government's priorities will need to be regularly reviewed and updated to respond to emerging challenges and rapid technological changes arising from the use of personal data. A power to designate a statement allows for the

government's priorities to be periodically reviewed and for the priorities set out in that statement to be transparently amended where necessary in accordance with the review procedure set out in new section 120G of the DPA 2018.

Justification for the procedure

79. The government considers that the statement of strategic priorities should be subject to a parliamentary procedure akin to the negative resolution procedure before it can be designated by the Secretary of State. This is considered to provide the appropriate level of parliamentary scrutiny for this type of statement because whilst the statement is intended to provide helpful context for the Information Commissioner and the Commissioner will be required to have regard to the priorities set out in the statement, there is no requirement to act in accordance with them.

80. There is precedent for the use of this procedure for government strategic priority statements. For example, the same procedure is applied to the statement of strategic priorities which may be designated under section 2A of the Communications Act 2003 by virtue of section 2C(5) of that Act. This parliamentary procedure also applies to the statement which the Secretary of State may publish under section 2A of the Water Industry Act 1991 setting out strategic priorities and objectives for the Water Services Regulation Authority (see section 2A(6) of that Act).

81. It is noted that in some cases, the affirmative resolution procedure applies in relation to government strategic policy statements. In particular, this procedure is applied to the statement which the Secretary of State may designate under section 4A of the Political Parties, Elections and Referendums Act 2000 (PPERA) by virtue of section 4C(8) of that Act (inserted by section 16 of the Elections Act 2022). The affirmative procedure also applies to the strategy and policy statement which may be designated by the Secretary of State under section 131 of the Energy Act 2013 (see section 135(8) of that Act). The statement of strategic priorities under new section 120E of the DPA 2018 can be differentiated from these statements because it is more limited and may not set out any particular role for the Information Commissioner in achieving the government's data protection priorities or require the Commissioner to exercise functions in a manner calculated to achieve particular outcomes. We therefore consider that it is appropriate for a procedure akin to the negative resolution procedure to apply to the statement made under new section 120E.

Clause 31(2): Power to require the Information Commissioner to prepare codes of practice for data processing

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Negative procedure

Context and Purpose

82. Section 128 DPA 2018 provides a power for the Secretary of State to make regulations requiring the Information Commissioner to prepare codes of practice giving guidance as to good practice in the processing of personal data and to make them available to such persons as the Commissioner considers appropriate. Any code of practice required to be issued under regulations made under section 128 would be in addition to the four topic-specific codes that the Information Commissioner is required to produce under section 121 to 124 DPA 2018. Where a code of practice is issued under section 121 to 124, the code is subject to additional requirements in section 125 to 127 DPA 2018 which set out the process for approval of those codes, requirements for publication and review of the codes and the effect of the codes.

83. Clause 31 replaces section 128 DPA 2018 with new section 124A, restating the Secretary of State's existing power to make regulations requiring a new code of practice to be produced and requiring consultation with the Secretary of State and other relevant persons on the code. It also provides that where a new code of practice is required by regulations, that code of practice will be subject to the same parliamentary approval process, requirements for publication and review and have the same legal effect as other codes of practice issued under section 121 to 124. This is intended to remedy the discrepancy between codes of practice issued under section 121 to 124 and those that may be required by regulations.

84. As for other codes of practice, codes issued under new section 124A will also be subject to new requirements inserted into the DPA 2018 by clauses 32 and 33 to establish a panel to consider the code, prepare an impact assessment on the code and to submit the code to the Secretary of State for approval.

Justification for taking the power

85. This is a restatement of the Secretary of State's existing power to make regulations requiring the Information Commissioner to prepare a code of practice under section 128 DPA 2018 and the amendments made are intended to remedy the discrepancy between codes of practice issued under section 121 to 124 and those that may be required by regulations made by the Secretary of State. The power to require an additional code of practice through regulations has not yet been exercised by the Secretary of State, but remains necessary as there may be situations where, due to the evolution of new technologies or in response to societal pressure, additional codes of practice may be desirable to set out good practice and support data protection compliance.

86. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see section 182 DPA 2018).

Justification for the procedure

87. The existing regulation making power under section 128 DPA 2018 is subject to the negative resolution procedure and the power as restated in new section 124A will be subject to the same procedure. The negative procedure remains appropriate as any regulations made under this power will simply impose a duty on the Information Commissioner to provide practical guidance on good practice in the processing of personal data and the negative procedure affords the appropriate level of parliamentary scrutiny for this.

Clause 32:Power to disapply/modify requirements for panels to consider code of practice

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary procedure: Negative procedure

Context and Purpose

88. This clause inserts new section 124B into the DPA 2018 which requires the Information Commissioner to establish a panel to consider a code of practice which is prepared under section 121 to 124A of the DPA 2018 and submit a report on the code to the Commissioner. The panel should be made up of individuals with relevant expertise and those who are most likely to be affected by the code. The Information Commissioner is required to publish a statement identifying the members of the panel and the process for selection. The Commissioner is also required to make arrangements for members of the panel to consider the code with one another and prepare and submit a report on the code to the Commissioner.

After the report has been submitted, the Commissioner must make any alterations to the code that are considered to be appropriate in light of the report and publish the code in draft along with the report (or a summary of it). Where a recommendation in the report has not been accepted by the Commissioner, an explanation of why it has not been accepted should be published.

89. Subsection (11) of new section 124B allows the Secretary of State to make regulations disapplying or modifying the requirements of new section 124B in the case of a code which the Commissioner is required to prepare under regulations made under new section 124A (as such this is a limited Henry VIII power). This is because, whilst we anticipate that the panel consultation requirements will ordinarily apply to a new code prepared under new section 124A, it may not be feasible or proportionate for all of these requirements to apply to every new code of practice which the Secretary of State requires the Commissioner to prepare under this section. For example, it may be that due to the nature of the matter covered by the code it would not be appropriate for an external panel of experts to consider the code or it may not be appropriate to identify individual panel members.

Justification for taking the power

90. This power is needed as it is not possible to anticipate what codes of practice may be required by regulations made under section 124A because, as set out above, this will depend on the evolution of new technologies or emerging societal issues that need to be addressed. It is therefore not possible to anticipate now whether it will always be appropriate to apply the new requirements for a panel consultation to that code and a power to disapply or modify the new section 124B requirements is needed to allow for this decision to be taken at the time that a new code of practice is required based on the proposed topic of the code.

91. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see section 182 DPA 2018).

Justification for the procedure

92. The negative resolution procedure is considered to be appropriate for regulations made using this power as the regulation making power may only be used to disapply or modify the new section 124B requirements in relation to codes of practice required by regulations made under new section 124A. Regulations requiring a code to be produced under new section 124A are subject to the negative resolution procedure and before a code takes effect it will be laid before Parliament and be subject to a parliamentary procedure akin to the negative resolution procedure in accordance with section 125(3) of the DPA 2018. It is considered that it is appropriate for the same level of scrutiny to apply to regulations disapplying or modifying the panel consultation requirements for that code. There is no power to disapply or modify the panel consultation requirements for codes of practice which the Information Commissioner is required to produce under section 121 to 124 of the DPA. In addition, only the requirements in new section 124B relating to a panel consultation on a new code of practice may be disapplied or modified using this power. Where such powers are used, the code would continue to be subject to scrutiny through requirements in new section 124A(4) of the DPA 2018 to consult the Secretary of State and other relevant persons on the code, requirements in new section 124C to prepare and publish an impact assessment on the code and requirements in new section 124D to submit the code to the Secretary of State for approval.

Clause 41 : Power to require controllers to notify Information Commissioner of the number of complaints received
Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Negative procedure

Context and Purpose

93. This clause inserts new section 164B into DPA 2018, giving a power to the Secretary of State by regulations to require a data controller to notify the Information Commissioner of the number of complaints made to it under new section 164A. (Section 164A requires data controllers to respond to and make enquiries into the subject matter of complaints from data subjects relating to an infringement of the processing of their personal data.)

94. This provision is part of the government's overall data reform package, which aims to give the Information Commissioner the ability to take a more risk-based approach to complaints and, where possible, to devote fewer resources to low impact complaints in favour of more upstream, preventative regulatory activity. This provision gives the Secretary of State the power - if attempts to encourage data controllers voluntarily to report complaints are unsuccessful - to require transparency from controllers regarding the number of complaints they receive, enabling the Commissioner more easily to monitor the volume of complaints data controllers are receiving over a specified period of time.

Justification for taking the power

95. It is important for the Secretary of State to be able to impose reporting requirements on controllers via secondary legislation; in particular, the government envisages imposing different thresholds for the notification of complaints to the Commissioner on different categories of controllers (large controllers, and controllers in certain data-intensive sectors, for example, may be subject to different notification thresholds from some smaller controllers). In the first instance, the intention is to set out a non-legislative route to encourage controllers and organisations to report their own complaints volumes to the Information Commissioner (on a voluntary basis), and then to exercise the power to make regulations only if the non-legislative route does not give the results required (e.g. if insufficient numbers of data controllers report on their complaints). At that stage (assuming voluntary reporting has not yielded the information required), the Information Commissioner would be likely to have a clearer idea of which sectors it should target for reporting purposes: for example, controllers which process a large quantity of data, or particularly sensitive, personal data, may be subject to different notification thresholds or required to always make a notification (regardless of the number of complaints they receive). The Information Commission will also be in a better position, at that point, to specify the form and manner of notification (including the relevant reporting periods).

96. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see section 182 DPA 2018).

Justification for the procedure

97. By virtue of new section 164B(5), this power is subject to the negative procedure. Controllers will simply be required to provide a figure (the relevant number of complaints received) to the Commissioner so this is not an overly onerous burden. Nor should such an obligation be controversial: a key principle of the data protection legislative framework is that data protection is processed lawfully, fairly and in a transparent manner, and the publication of the number of complaints received from data protection subjects is likely to

support (in particular) the third limb of this principle. The negative procedure therefore affords the appropriate level of parliamentary scrutiny for the exercise of this power.

Clause 49(1): Power to prepare the digital verification services (DVS) trust framework

Power conferred on: Secretary of State

Power exercised by: Document

Parliamentary Procedure: None

Context and Purpose

98. Clause 49(1) confers a duty on the Secretary of State to prepare and publish the DVS trust framework, a document setting out the rules that digital verification services organisations must follow when providing verification services under Part 2. Under subsection (3) of clause 49 the Secretary of State must consult the Information Commissioner and anyone the Secretary of State thinks appropriate when preparing this document. Under subsection (4) the requirement to consult can be satisfied by the consultation being undertaken before the coming into force of the clause. The Secretary of State must carry out a review of the DVS trust framework at least every 12 months and in doing so must consult the Information Commissioner and anyone the Secretary of State thinks appropriate The Secretary of State may revise and republish the DVS trust framework following such a review or following an informal review. The DVS trust framework or a revised version of the framework comes into force when it is published unless a different commencement date is specified. Different commencement times for different purposes can be specified in the DVS trust framework and it can include transitional provisions and savings. Clause 50 requires the Secretary of State to establish and maintain a register of organisations providing digital verification services. Clause 50(4) provides that where an organisation holds a certificate from an accredited conformity assessment body certifying that the digital verification services provided by the organisation comply with the DVS trust framework and the organisation makes a proper application to be included in the register and pays the required fee, the Secretary of State must include that organisation in the register unless the organisation has already been removed from the register for specified period under clause 54 and is seeking to be re-registered during that period.

Justification for taking the power

99. The DVS trust framework document will set out in detail the rules and technical industry standards that digital verification services organisations are required to follow when providing verification services. The document will also cover technical guidance to facilitate interoperability between organisations providing digital verification services; industry standards and best practice for encryption and cryptographic techniques, quality management systems, information management, information security, risk management, fraud management; guidance for dealing with fraud, service delivery or data breaches; guidance for dealing with complaints and disputes and record keeping and record management. Since the DVS trust framework will be concerned with complex technical industry standards as well as administrative matters, it would not be appropriate to set out this type of detail in legislation. Accredited conformity assessment bodies will be responsible for certifying organisations against the DVS trust framework and will provide complex technical oversight . Under clause 53 if the organisation no longer holds a certificate from an accredited conformity assessment body certifying that they are providing digital verification services in accordance with the trust framework, the Secretary of State must remove the organisation from the register. Under clause 54 if the organisation is failing to provide digital verification services in accordance with the DVS trust framework, the Secretary of State may remove the organisation from the register.

Justification for the procedure

100. As the DVS trust framework is concerned with technical matters, no Parliamentary procedure is considered necessary. The duty to review the framework at least every 12 months and duty to consult as well as the power to revise and republish the framework following a review or informally provides the ability to modify and adapt the framework promptly if changes are required to ensure organisations are being assessed against the most up to date rules and industry standards. Industry standards relating to the provision of digital verification services can change frequently and if an industry standard contained in the DVS trust framework is revised, for example to reduce a threat to security or privacy, the DVS trust framework would need to be rapidly updated to take account of this. It is important to have the ability to amend the reference to any standard in an appropriately timely fashion. For example, if a particular encryption standard were found to be no longer fit for purpose in ensuring data security or in mitigating cyber risks, the DVS trust framework rules would need updating in rapid time. Such action will be necessary to maintain the credibility of the trust framework with actors in the digital identity ecosystem who will be aware of the industry standards changing and will expect the DVS trust framework to keep reflecting these appropriately. Under clause 63(1) of the Bill the Secretary of State may make arrangements for a third party to exercise her functions under Part 2 of the Bill. The governance of the trust framework will sit within the Department for Science, Innovation and Technology initially and it is possible the Secretary of State will delegate the powers in relation to the trust framework to another public sector body, a regulator or to the private sector in future. If these powers were delegated to a private sector entity, it would be inappropriate to require the trust framework to be set out in regulations subject to parliamentary scrutiny, as the regulation-making power could not be exercised by a non-governmental body. The approach under Clause 49 will ensure that governance of the digital identity ecosystem remains portable outside of the Department.

Clause 52(1): Power to make a determination that a fee must be paid to the Secretary of State by a DVS provider for registration in the DVS register

Power conferred on: Secretary of State
Power exercised by: Ministerial Determination
Parliamentary Procedure: None

Context and Purpose

101. Clause 52(1) provides a power for the Secretary of State to make a determination that a provider who applies to be registered in the Digital Verification Services (DVS) Register ("the Register") must pay a specified fee. Subsection (3) of the clause allows the Secretary of State to determine that DVS providers who are already registered must pay a specified fee at such a time as is listed in the determination. Subsections (2) and (4) of the clause provide that the Secretary of State can set fees in excess of the administrative costs associated with applications for registration and continued registration. Subsection (6) provides that a determination may make different provisions for different purposes. For example, a fee could be set at a higher level for a certain type of digital verification service provider. The Secretary of State is required to publish a determination setting the fees that are payable under this scheme under subsection (7). Subsections (8) and (9) allow the Secretary of State to revise fees, and require any revised fees to be published.

102. Under clause 63(1), the Secretary of State may make arrangements for a third party to exercise the Secretary of State's functions under Part 2 of the Bill. The governance of the UK's digital identity ecosystem, including the UK digital identity and attributes trust framework, will sit within the Department for Science, Innovation and Technology for an

interim period, while a permanent location is sought for governance to sit as the market develops and matures. It is possible that the Secretary of State will delegate these governance powers outside of the department to another public sector body, a regulator or to the private sector in future. If these powers were delegated to a private sector entity, it would be inappropriate to require fees to be set in regulations which are subject to parliamentary scrutiny, as this regulation-making power could not be exercised by a non-governmental body. Setting the fees by way of a determination will therefore ensure that governance of the digital identity ecosystem remains portable outside of the department. Clauses 52(7) and (9) require any determination to be published, ensuring the fee structure is transparent.

Justification for taking the power

103. The fee structure to be set is likely to be technical and complex, with different fees to be applied for different purposes as permitted by subsection (6). The fees can be set at a level which goes beyond purely recovering costs of administering the application to join or remain on the register itself. If the fee were set at such a level as to go beyond cost-recovery, additional revenues are intended to fund wider governance functions necessary to operate the market. The digital identity market is nascent and the level of fees may need to be adjusted from time to time to keep pace with changes in the market, therefore there needs to be the ability for the Secretary of State to adjust the fee structure fairly and appropriately. Giving the Secretary of State this power to set fees by determination will help to ensure that the government is able to respond swiftly to changes in the market, balance the interests of industry and the taxpayer, and support growth in this evolving market. The voluntary nature of this regime, and the desire to grow this market in a sustainable and inclusive way, means there is a strong incentive for the Secretary of State to set any fees at a level that is competitive, fair, and reasonable. There will be very little incentive for the Secretary of State to set excessively high fees, as to do so would prevent the government from realising its ambitions to grow this market. It would be overly restrictive to commit this fee regime to primary or secondary legislation.

Justification for the procedure

104. Entry onto the DVS Register is not mandatory for those wishing to provide digital identity services in the UK. However, entry onto the Register does confer certain advantages, notably that a public authority may only disclose information to a DVS provider which is on the Register under clause 56. The fees that can be charged under clause 50 form part of this non-compulsory scheme which private, commercial entities can choose to partake in to provide a commercial service to their users. It is appropriate in this scenario for the fee structure to be set out by way of determination rather than primary or secondary legislation, as this legislation does not establish a compulsory regulatory regime and the determination will not impose an obligation on any person. The government considers that publication of the Secretary of State's determinations on fees, as required under clauses 52(8) and 52(9), provide an appropriate level of scrutiny and transparency to this fee regime. If in exercising the powers under clause 63(1), the power to set fees was delegated to a private sector entity, it would be inappropriate to require the fees to be set out in regulations subject to parliamentary scrutiny, as the regulation-making power could not be exercised by a non-governmental body.

105. Insofar as the power could be considered legislative, its scope is limited: the power merely permits the Secretary of State to set the amount or amounts of fees for entering or remaining on the Register. These factors all restrict the Secretary of State's power in determining fees to a level that means Parliamentary procedure is not necessary for further scrutiny of the power.

Clause 60(1): Power to prepare and publish a code of practice about the disclosure of information

Power conferred on: the Secretary of State

Power exercised by: Statutory Code of Practice

Parliamentary Procedure: Affirmative procedure (negative procedure where the Code is republished).

Context and Purpose

106. This clause requires the Secretary of State to prepare and publish a code of practice about the disclosure of information by public authorities to persons registered in the digital verification services register. It provides that a public authority must have regard to the code of practice in disclosing information relating to an individual for the purposes of enabling an organisation to provide digital verification services for the individual under clause 56.

107. The code must be consistent with the data sharing code of practice prepared by the Information Commissioner under section 121 DPA 2018 and issued under section 125(4) of that Act. The Secretary of State is able to revise and republish the code from time to time and when doing so, must consult the Information Commissioner and any other persons the Secretary of State thinks appropriate. The consultation requirement may be satisfied by consultation undertaken before the coming into force of this clause.

Justification for taking the power

108. The code will provide guidance to public authorities on disclosing information to an organisation for the purpose of providing digital verification services to an individual. The code will provide practical guidance on the use of the powers in a way that is consistent with the data sharing code prepared by the Information Commissioner. The Code does not create any new legal obligations.

109. In this context, it is appropriate for the power to be conferred on the Secretary of State and there are appropriate safeguards, such as the requirement for consultation before preparing or revising the code, which will contribute to ensuring that the code is drafted to a high standard. There is also strong precedent for powers to be taken for preparing and publishing codes of practice such as the code issued under section 43 of the Digital Economy Act 2017.

Justification for the procedure

110. Publication of the first version of the code will be subject to the affirmative procedure and require approval by both Houses of Parliament, before laying. Republication of the code will be subject to the draft negative procedure with a requirement that before republishing the code a draft is laid before Parliament. Any republication of the code will not become law if either House resolves not to approve it within 40 days.

111. The code provides practical guidance to public authorities on the disclosure of information, including on matters such as data minimisation. It is considered that given the nature of the code, this procedure provides an appropriate level of Parliamentary scrutiny.

Clause 63(1): Power to make arrangements for third party to exercise functions

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

112. This clause enables the Secretary of State to make arrangements for a person prescribed by regulations to exercise the functions of the Secretary of State under Part 2.

Justification for taking the power

113. The clauses in Part 2 establish a new, non-compulsory scheme for digital verification services and include governance functions conferred on the Secretary of State in order to secure the reliability of digital verification services. The Secretary of State's governance functions and the restrictions on the exercise of those functions are set out on the face of the Bill. These functions include a duty to prepare and publish the DVS trust framework (clause 49); a duty to establish and maintain a public register of DVS providers (clause 50); powers to determine how applications to the register should be made and what fees should be paid (clauses 51 and 52); powers to remove DVS providers from the register (clauses 53 and 54); a duty to prepare and publish a code of practice about the disclosure of information by public authorities (clause 60); a power to designate a trust mark for use by registered DVS providers only (clause 61); a power to require accredited conformity assessment bodies or registered DVS providers to provide information to the Secretary of State (clause 62); a duty to prepare and publish a report on the operation of the scheme (clause 64). The responses to the public consultation identified that the governance of the UK's digital identity ecosystem, including the UK digital identity and attributes trust framework should sit within the Department for an interim period while the market is developing. During this period the Secretary of State will need to react to the governance needs of the nascent digital identity market when deciding how and whether to exercise this power. It is not yet clear where the most appropriate permanent location for these functions should be when the market is larger and more mature. In recognition of this evolving situation, the government considers the Secretary of State should be able to delegate these governance functions if it becomes appropriate to do so.

114. It would be overly restrictive to identify a particular third party or to define a set of circumstances in which the Secretary of State should exercise the power under clause 63 to delegate functions under Part 2. This could lead to a situation where the governance needs of the digital identity market are not properly met, preventing the government from realising its ambitions to grow this market in secure and trusted digital verification services. But in the future, it is possible that the Secretary of State will consider that trust and security can be better achieved by delegating these governance functions outside of the Department to another public sector body, a regulator or to the private sector.

Justification for the procedure

115. The regulations are subject to the affirmative procedure. This is considered appropriate given the nature of the functions to be delegated. While certain functions are administrative and operational in nature, for example, the duty to establish and maintain a register of digital verification services providers, there are functions, such as the duty to set the rules of the trust framework and the power to remove digital verification services organisations from the verification services register, that are substantive functions. Parliament should therefore have the opportunity to scrutinise and debate the proposed arrangements for another person to take on these functions. It is considered that the affirmative procedure provides the appropriate level of scrutiny.

Clause 66(1)-(3): Power to require suppliers of goods or services to provide their customers with improved access to their transactional data (smart data schemes)

Power conferred on: Secretary of State and the Treasury

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure (apart from some amendment regulations)

Context and Purpose

116. Part 3 of the Bill implements a government commitment, made further to a public consultation (Smart data: putting consumers in control of their data and enabling innovation[3]) in 2019, to obtain powers to introduce "smart data schemes" in markets across the economy. The objective is to improve data portability (beyond the limited right to data portability in the UK GDPR, where it applies) between suppliers, their customers and representatives authorised by the customer to help overcome information asymmetry between suppliers and their customers, to enable customer access to data in "real time" and to facilitate better use of customer data for instance to enable customers to compare deals and switch suppliers.

117. Part 3 of the Bill comprises several clauses containing regulation-making powers. Aside from this clause 66 (power to make provision in connection with customer data), there are regulation-making powers in clauses 68 (power to make provision in connection with business data), 71 (enforcement of data regulations), 74 (fees) and 75 (levy). These are explained further below, but as the regulation-making powers in those clauses ensure the effectiveness of smart data schemes, the explanation for this clause 66 is also relevant in considering those clauses.

118. The "principal" power in subsection (1) of this clause 66 allows the Secretary of State or the Treasury, by regulations, to require suppliers of goods, services and digital content specified in the regulations and other persons holding the relevant data (collectively, "data holders") to provide customers or their authorised representatives with access to customer data. Customers (see clause 65(3)) may include both consumers and business customers; small and medium enterprises face many similar disadvantages arising from their ability to access data as consumers. Customer data (clause 65(2)) includes data relating to the goods, services or digital content provided to the customer and the price paid. It is intended that the regulations will require the provision of data to customers' authorised representatives, but the powers also allow for provision of data directly to customers.

119. Subsections (2) and (3) provide "ancillary" powers which ensure that the "principal" power in subsection (1) can be effective. Subsection (2)(a) confers a power to require suppliers to collect and retain data, to ensure they have specific and accurate data to hand for disclosure. Subsection (2)(b) confers a power to provide for rectification of inaccurate data (this is necessary as not all customer data will be personal data to which the UK GDPR rectification right applies). Subsection (3) confers a power to allow the authorised representative to exercise the customer's rights in relation to the goods, services or digital content supplied or provided by the supplier (action initiation: see paragraph 124a).

120. Clause 67 illustrates how the regulation-making power may be used. That includes provisions for the following purposes: requests to access data (subsection (2)); customer authorisation of representatives to access data or act on the customer's behalf (subsection (3)); how and when the data may be accessed or provided (subsection (4)); collation and retention of records relating to provision of and access to data (subsection (5)); imposing obligations on third parties to assist the supplier in complying with its obligations (subsection

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

(6)); onward processing and disclosure of the data (subsection (7)); making customers aware of their data rights (subsection (8)); complaints and disputes resolution (subsections (9) and (10)). Other ancillary clauses include clauses dealing with: the appointment of decision-makers (clause 70), to accredit persons who customers may authorise to receive customer data on their behalf (see clause 67(3)(b)); enforcement (clauses 71, 72 and 73, which are explained in more detail below); powers to enable the charging of fees (clause 74) and the imposition of a levy (clause 75) (both of which are also explained below) and a spending authority (clause 76).

121. Part 3 of the Bill replaces the existing regulation-making powers in sections 89-91 (supply of customer data) of the Enterprise and Regulatory Reform Act 2013 ("ERRA") which enable the Secretary of State to make regulations to require the suppliers of goods or services (see section 89(2)) to provide customer data to a customer or to another person authorised by the customer at the customer's or authorised person's request. The ERRA powers were introduced as a backstop should it not be possible for suppliers to develop voluntary programmes for the release of data to customers. The Department for Business, Innovation and Skills explained those powers in an Addendum to the delegated powers memorandum for that Bill (see the Committee's 14th Report for session 2012-13). Experience to date has shown that industry has not voluntarily put in place such programmes and therefore regulation powers remain necessary.

Justification for taking the power

122. The essential purpose of Part 3 is to update the government's regulation-making powers to allow the government to establish effective smart data schemes. In doing so, the government would like to maintain general regulation-making powers building on those enacted in ERRA. Regulation-making powers of this kind allow the government to tailor each scheme to the circumstances of the sector to which it applies in respect of which provisions, such as the data to which the scheme applies, the persons on whom obligations are imposed and how data may be requested and accessed, may necessarily be detailed and vary. Furthermore, the government considers that seeking primary legislation for the establishment of each specific smart data scheme would significantly limit the feasibility of introducing such schemes. At present, smart data schemes are in contemplation in the areas of financial service markets (expanding or replacing the open banking scheme which was introduced by order of the Competition and Markets Authority under its competition powers) and in retail telecoms, such as fixed line broadband and mobile services. A common framework of powers may also facilitate cohesion between smart data schemes for instance in terms of their interoperability.

123. It is not intended to alter fundamentally the activities to which the powers may apply, as compared with ERRA. The regulation-making powers will allow regulations to be made in the context of the provision of goods, services or digital content specified in the regulations, which is intended to replicate the scope of ERRA section 89(2)(d) (the reference to digital content is added to reflect Part 1 of the Consumer Rights Act 2015 which contains separate provisions for the supply of goods, digital content and services). However, the ERRA powers are no longer adequate to enable the introduction of regulations with all the features required to be effective. Since 2013, the government's understanding of what is required for a successful smart data scheme has evolved because of the open banking scheme, which was introduced by order of the Competition and Markets Authority (CMA) under its competition powers in Part 4 (market studies and market investigations) of the Enterprise Act 2002 following a CMA market study in relation to competition within the retail banking market. The open banking scheme enables customers to share their bank and credit card transaction data securely with trusted third parties who can provide them with applications and services. The government has also had regard to the recent enactment of powers in Part 4 of the Pension Schemes Act 2021 (which amends the Pensions Act 2004 and the Financial Services and Markets Act 2000) for pensions dashboards, an electronic communications service for individuals to access information about their pensions.

124. Aside from the extension of the regulation-making powers to contextual business data (which is dealt with in clause 68), key changes (as compared with ERRA) include:

a. Action initiation (see clause 66(3)): this allows an authorised representative to act on the customer's behalf in exercising the customer's rights in relation to the goods, services or digital content supplied or provided by the relevant supplier: for instance, the regulations might provide for the representative to access the customer's account and make a payment or to negotiate an improved deal on the customer's behalf. This proposal is based both on the experience in Australia with its Consumer Data Right, where action initiation (write access) provisions are being introduced to realise the full potential of smart data use cases, such as enabling more efficient switching of suppliers, and on the read and write access standards adopted under the UK's open banking scheme, and is critical to allow customers to be able to achieve tangible benefits from the improved access to their customer data.

b. Technical requirements (clauses 67(4)(b) and (7)(a) and 78(1)(f)): to be effective, smart data schemes rely on the secure transfer of customer data in usable formats. Accordingly, data holders, and those requesting and receiving data, may be required to participate in facilities and services, and comply with associated requirements, including electronic communication services such as application programme interfaces.

Given the complicated and technical nature of these IT focused requirements, and the need for their rapid update, it is essential that the powers allow for appropriate sub-delegation of rule-making as is permitted by clause 78(1)(f) which allows the regulations to make provision by reference to specifications or technical requirements published from time to time by a specified person. Clause 78(1)(f) reflects section 238A(5)(a) of the Pensions Act 2004 under which regulations may require the pensions dashboards service to comply with standards, specifications or technical requirements published from time to time by the Secretary of State, the Money and Pensions Service or another person specified, or of a description specified, in the regulations.

While largely reenacting section 91(1)(b) of ERRA, clause 78(1)(g), which allows the conferral of functions on a person including functions involving the exercise of a discretion, may also be necessary to facilitate the functioning of technical requirements as well as in other contexts in which a discretion might reasonably be conferred (for instance in relation to the accreditation of persons who may be authorised by a customer (clause 67(2)), the resolution of complaints or disputes (clause 67(9) and (10)) or in relation enforcement decisions and the imposition of fees or the levy which are explained further). Clause 78(1)(g) is again similar to the provision made in relation to pensions dashboards by section 238A(6) of the Pensions Act 2004 in which regulations may include provisions for determinations to be made by the Secretary of State, the Money and Pensions Service, or another person specified, or of a description specified, in the regulations.

c. Assistance: given that the provision of goods, services and digital content, and the processing of data in relation to it, can involve multiple parties, in addition to a broad definition of "data holder" (clause 65(2)), clause 67(6) introduces an express power to require other persons to assist the supplier in complying with the regulations.

d. Data processing (see clause 67(7): it is considered prudent to introduce powers, not contained within ERRA, to impose obligations on the processing

and further disclosure of data should the government consider this necessary to protect the interests of customers.

e. Enforcement (see clauses 71, 72 and 73): the ERRA powers are inadequate to allow for effective enforcement of smart data schemes; the enforcement provisions are explained separately.

f. Funding (see clauses 74 and 75): it is intended that the regimes introduced by regulations should be "self-funding" which is not achievable under ERRA; the relevant clauses are explained in more detail. There is also a back-stop spending authority to allow the government to provide financial assistance to persons exercising functions under a smart data scheme (clause 76), but it is not anticipated that the government will make regular use of this authority.

g. Several ancillary provisions are introduced including powers to require data holders to publish information to make customers aware of their rights (clause 67(8)) and for complaint and dispute resolution provisions (clause 67(9) and (10)).

h. Confidentiality and data protection: Part 3 introduces specific provisions, reflecting the pensions dashboards provisions in section 238B(6) and (7) of the Pensions Act 2004, on the relationship of the regulations with data protection legislation (clause 77).

125. These changes are balanced by significant strengthening of safeguards on the making of regulations, as compared with ERRA. Aside from the Parliamentary scrutiny of regulations (which is addressed in paragraphs 126-128), the regulation-making powers now require:

a. Substantive preconditions (see clause 66(4)): in deciding whether to make regulations, the regulation-maker must consider a number of specified matters. This applies to all regulations: by contrast, the statutory preconditions for exercise of the ERRA powers do not apply in the case of regulations under section 89(2)(a)-(c) (supply of gas or electricity, mobile phone services and provision of current accounts and credit card facilities) and only apply in the case of other goods or services (section 89(2)(d)) (see section 89(7)) (as a result of the application of the conditions, and affirmative scrutiny, to all first regulations about a particular description of customer data, the distinction between the goods and services in subsections (a)-(d) of section 89(2) is not replicated in the new powers).

b. Consultation (see clause 78(5)): there is a requirement of prior consultation of persons likely to be affected by the regulations and sectoral regulators on all regulations which are subject to affirmative scrutiny.

c. Periodic review (see clause 79): there is a requirement for a periodic review of regulations, against the substantive preconditions, at least every five years and ministers must publish the outcome of that review and report it to Parliament. This is intended to ensure that smart data schemes are kept under review and is designed to align, in practice, with any review under sections 28 to 32 (secondary legislation: duty to review) of the Small Business, Enterprise and Employment Act 2015 where they apply.

Justification for the procedure

126. The affirmative resolution procedure is required in the case of the first regulation making provision under clause 66(1)-(3) about a particular description of customer data (see clause 78(3)(a)). This is designed to ensure that Parliament has an opportunity to debate the

regulations whenever a smart data scheme, or provision of the kind in clause 68(1) and (2), is first introduced. By contrast, the ERRA powers only require the affirmative resolution procedure in the case of regulations to which section 89(2)(d) applies and for regulations containing enforcement provisions.

127. Subsequent regulations must also be subject to the affirmative resolution procedure (see clause 78(3)(c)-(e)) where those regulations:

a. make the requirements of existing regulations more onerous for data holders;

b. contain enforcement or investigatory provisions;

c. contain revenue-raising provisions;

d. amend or repeal primary legislation: clause 78(2) contains Henry VIII powers for the amendment or repeal of primary legislation in the case of provisions about the handling of complaints, dispute resolution, appeals and provisions under clause 78(1)(h) (incidental, supplementary, consequential, transitory, transitional or saving provisions) the principal purpose of these powers being to enable regulations to extend, adapt or apply existing statutory complaints, disputes and appeals processes for the purpose of a smart data scheme and to make such consequential amendments as allow the scheme to function effectively.

128. It is, however, considered appropriate for other subsequent regulations to remain subject to negative Parliamentary scrutiny.

129. These requirements, coupled with the requirements of consultation and periodic review, represent a significant strengthening of the procedural requirements as compared with ERRA and a counterbalance to the new provisions sought.

Clause 68(1) & (2): Power to require suppliers of goods or services to publish, or provide their customers with access to, contextual information about their goods and services

Power conferred on: Secretary of State and the Treasury

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure (apart from some amendment regulations)

Context and Purpose

130. Subsection (1) ensures that suppliers of goods, services or digital content may be required to provide, or publish, wider information about the goods, services and digital content they provide that does not relate to individual customers (business data). This business data may include information on the availability of the supplier's goods or services (for instance, geographic coverage), tariffs, key contractual terms and data on customer feedback.

131. The publication or provision of wider business data is necessary to allow customers and their representatives, and other parties including prospective customers, to understand the relevant market and allows customers to contextualise any customer data provided to them. This may, for instance, allow customers to compare alternative deals best suited to their means and needs.

132. As with clause 66(2)(a) in relation to customer data, subsection (2) provides a power to require suppliers to collect and retain specific kinds of business data. Clause 69 illustrates how the regulation-making power may be used and substantially mirrors clause 67.

133. The powers in clause 68 may be used in conjunction with a smart data scheme under clause 66 or separately.

Justification for taking the power

134. The ERRA powers do not extend to business data, so it is necessary to expand regulation-making powers to cover this kind of data. In doing so, clause 68(1) and (2) substantially replicate clause 66(1)(a) (with the modification that it is not necessary for a third party recipient to be authorised by the customer, since business data does not relate to a specific customer) and (2)(a).

135. The government considers, in relation to the kind of powers proposed in clause 68, that the same justifications apply as for clause 66: these being an ability to tailor regulations to the circumstances of the sector in question, that it is not feasible to seek primary legislation for each specific regulatory scheme and to facilitate cohesion between schemes.

Justification for the procedure

136. The power to make regulations relating to business data is subject to the same parliamentary procedures in the same cases as those proposed for customer data as explained in the context of clause 66 so that the affirmative resolution procedure is required in the case of the first regulation making provision under clause 68(1) and (2) about a particular description of business data (clause 78(3)(b)) and for subsequent regulations of the kind in clause 78(3)(c)-(e). The government considers that this level of scrutiny, the statutory conditions for making regulations and the requirements of consultation and periodic review provide appropriate safeguards, constraints and scrutiny on use of this power.

Clause 71(1): Enforcement of smart data schemes

Power conferred on: Secretary of State and the Treasury

Power exercised by:Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

137. This clause 71(1) provides powers for the enforcement provisions of the smart data regulations.

138. Enforcement will be by a public body identified in the regulations (subsection (1)). The regulations may provide for more than one enforcer and, if so, for the relationship between them (subsection (11)).

139. The regulations may confer investigatory powers on the enforcer (subsection (3)) but these are subject to restrictions in clause 68 (an enforcer may not enter a private dwelling without a warrant and there are restrictions on the information that the regulations may require a person to provide an enforcer, notably to maintain the privileges of Parliament, to maintain legal privilege and, subject to exceptions, to protect against self-incrimination).

140. In the case of infringement of the regulations or requirements imposed under them, an enforcer may issue a notice requiring compliance with the data regulations or conditions or requirements imposed under them (compliance notice) (subsection (4)(a) and (b)).

141. In the case of infringement of the regulations, or of a failure to comply with a compliance notice or the provision of false or misleading information, the regulations may provide for an enforcer to impose a financial penalty (subsection (6)). An enforcer's powers

to do so are subject to the safeguards in clause 73: inter alia, that clause provides that the amount of a financial penalty must be specified in, or determined in accordance with, the regulations (subsection (2)); it imposes procedural safeguards requiring an enforcer to issue guidance as to the exercise of any discretion provided by the regulations (subsection (3)(a)), and to provide persons on which the enforcer proposes with notice of the proposed penalty and an opportunity to make representations (subsection (3)(b)-(e)).

142. The regulations may contain review and appeal rights (clause 71(7) and must provide for appeals in the case of imposition of a financial penalty (clause 73(3)(f) and (g)).

143. An enforcer may also publish a statement that the enforcer considers that a person is not complying with the regulations or a compliance notice (clause 71(4)(c)) (this would allow "naming and shaming" in, for instance, persistent or egregious cases).

144. Clause 71(5) also allows for the creation of offences, punishable only with a fine, for the provision of false or misleading information or preventing an enforcer from accessing information or other material. These are designed to reflect broadly sections 144 and 148(2) DPA 2018.

145. For completeness, clause 70 allows a decision-maker to revoke or suspend the accreditation of a person to access data on behalf of customers which functions as a sanction in the case of non-compliance where an authorised representative is permitted to access data.

Justification for taking the power

146. The government considers that the kinds of sanctions which regulations may provide for, including powers to provide for both compliance notices and financial penalties, are necessary and appropriate to deal with infringements of, and incentivise compliance with, the regulations. Regulation-making powers under section 238G of the Pensions Act 2004 in relation to pensions dashboards allow regulations, among other things, to provide for the Pensions Regulator to issue compliance notices and impose financial penalties.

147. For the reasons explained in relation to clause 66 (customer data), it is considered necessary for the regulation-making powers under clause 66 and clause 68 to be framed as general powers which are applicable in a variety of contexts: it follows that the enforcement powers in clause 71 may be exercised in contrasting contexts. Accordingly, if sanctions are to be effective, it may be problematic for clauses 71 and 73 to specify, or limit, the amount of the financial penalties that may be imposed. However, both the investigatory powers (see clause 72) and the power to impose financial penalties (clause 73) are subject to statutory safeguards including the requirements that any financial penalties must include the procedural safeguards in clause 73(3) such as mandatory rights of appeal to a court or tribunal.

Justification for the procedure

148. All regulations containing enforcement provisions must be subject to the affirmative resolution procedure (clause 78(3)(d)), which mirrors section 91(3)(b) of ERRA, and consultation (clause 78(5)).

149. Regulations under this clause are also subject to mandatory periodic review (clause 79), including provision of a report to Parliament (clause 79(5)), as described for clause 66.

Clause 74(1): Power to allow charging of fees in smart data schemes

Power conferred on: Secretary of State and the Treasury

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

150. This clause 74(1) allows for regulations to provide that data holders, decision-makers, enforcers and other persons on whom duties are imposed or functions conferred by the regulations may require other persons to pay fees for the purpose of meeting expenses incurred (or to be incurred) by virtue of the regulations (subsections (1) and (2)).

151. Subsection (3)(b) provides that a fee can exceed the costs in respect of which it is charged: this is intended to ensure the efficacy and workability of the charging system, to allow the regulations to set fees by reference to "standard" amounts, or likely standard amounts, of costs rather than against the specific cost incurred in each particular case.

152. The amount of fees, or maximum amounts, must be specified in or determined in accordance with the regulations in the interests of certainty (subsection (4)). The regulations may allow for increases (subsection (5)) (that might be used, for example, to cater for inflation). Where a person has a discretion to determine the amount of a fee, that person must be required to publish information about the determination of that amount (subsection (6)).

Justification for taking the power

153. The principal objective of this clause 74, together with clause 75, 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, which cannot be achieved by the ERRA powers.

154. The clause also allows for provision for the charging of fees by data holders: while it is intended that the provision of data should be free to customers and their representatives, this clause would allow regulations to provide for charges for instance in the case of excessive and burdensome requests for data and is a reasonable safeguard in these cases.

Justification for the procedure

155. All regulations under this clause 74 are subject to the affirmative resolution procedure and public consultation (clause 78(3)(d) and (5)). It is considered that Parliament must have the opportunity to debate any regulations made under this clause bearing in mind the range of persons the clause might allow to impose, or require to pay, fees, the financial burden on those required to pay and the nature of the provisions that may be made under the clause.

156. Regulations under this clause are also subject to mandatory periodic review (clause 79), including provision of a report to Parliament (clause 79(5)), as described for clause 66.

Clause 75(1): Power to impose a levy on suppliers of goods or services to which a smart data scheme applies

Power conferred on: Secretary of State and the Treasury

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

157. Clause 75(1) allows regulations to impose, or provide for a specified public body to impose, a levy on data holders for the purposes of meeting expenses incurred by decision-makers and enforcers (subsection (1)(a)). Subsection (1)(b) allows the regulations to specify how funds raised may or must be used (this might allow a body collecting the levy to retain some or all funds or require it to provide funds to another body).

158. If the regulations provide for a specified public body to impose the levy, the regulations must provide how the rate of the levy and the period in which it is payable are to be determined (subsection (3)).

Justification for taking the power

159. The objective of this clause 75, together with clause 74, is to ensure that smart data schemes are "self-funding" and revenue-neutral to the exchequer which could not be achieved by the ERRA powers.

Justification for the procedure

160. All regulations under this clause 75 are subject to the affirmative resolution procedure and public consultation (clause 78(3)(d) and (5)), so that Parliament will have the opportunity to debate provisions for the levying of monies in the exercise of the powers of this clause.

161. Regulations under this clause are also subject to mandatory periodic review (clause 79), including provision of a report to Parliament (clause 79(5)), as described for clause 66.

Clause 83(3): Power to provide exceptions to the consent requirements for cookies and similar technologies

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

162. Current regulation 6 of Privacy and Electronic Communications (EC Directive) Regulations 2003 (the "PEC Regulations") sets out rules on the confidentiality of communications in "terminal equipment" such as computers, mobile phones, wearable technology, smart TVs and connected devices, including the Internet of Things. Regulation 6(1) prohibits the storing of information or gaining access to information stored in the terminal equipment of an individual (e.g. via the placement of cookies or similar technologies), unless the individual is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and the individual has given consent.

163. The government wishes to reduce the friction caused by numerous cookie consent pop ups, banners etc that are used on websites and apps to request user consent to cookies and similar technologies. The Bill will therefore introduce some limited exceptions to the requirements that user consent must be obtained for the use of cookies and similar technologies. The exceptions being introduced are considered to present a low risk to people's privacy. For example, clause 83(2), new paragraph 2A of regulation 6 introduces an exception that permits the storage of information, or access to information, for the purpose of collecting statistical information about how an organisation's information society service is used or provided, with a view to making improvements to that service. For example, statistical information showing how many people are accessing a service, what they are clicking on and for how long they are staying on a particular web page. Paragraph (2A)(c) provides a safeguard that prevents onward sharing of information except where the sharing is for the

purpose of making improvements to the service or website concerned. The exception applies only where the user is provided with clear and comprehensive information about the purpose and is given a simple and free means of objecting to the storage or access.The other exceptions are set out in clause 83(2), new paragraphs (2B), (2C) and (2D) of regulation 6.

164. Regulation 6A will introduce a power for the Secretary of State to amend the PEC Regulations by adding new exceptions to the cookie consent requirements. The power would also allow the Secretary of State to omit or vary any existing exceptions to the consent requirements as well as make consequential, incidental or supplementary provisions which are necessary to give effect to exceptions made by regulations made under these provisions.

Justification for taking the power

165. The government believes a new power is necessary as this is an area where technological advancements are constantly evolving and it is crucial to have a power safeguard and/or to amend regulation 6 to keep pace with the development. The power will ensure that the government is able to make changes to the exceptions to regulation 6(1) in the light of experience of how the exceptions operate in practice.

Justification for the procedure

166. These regulations will be subject to the affirmative procedure and include a duty to consult. This is considered appropriate given the exercise of the power could alter the scope of the exceptions to the consent requirement and what safeguards are in place to protect individuals' privacy rights.

Clause 83(3): Power to set requirements on suppliers and providers of information technology to enable users of technology to automatically consent or object to cookies and other similar technology when visiting websites

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

167. As outlined above, the Bill removes the need for consent to some forms of cookies and similar technologies that have a low impact on privacy. These changes mean that consumers can direct more of their time and attention to making important decisions about the use of cookies and other similar technology that may have a material effect on their privacy.

168. The government considers that the overall impact of the changes described above could be enhanced if users could express their privacy preferences through software (including browsers) and device settings. This would potentially remove the need for consent pop-up notices on each website or service, allowing individuals to express their privacy preferences on a single occasion and to have control over how these preferences are applied.

Justification for taking the power

169. At present, the technological options for expressing consent preferences in this way are limited and further work needs to be done with technology providers to increase the range of options available. The government considered including the detailed requirements for these online consent management tools on the face of the Bill. However, primary legislation

is not the best place to set out detailed technical specifications, when technology is continuously evolving in this area.

170. It has therefore been decided to introduce a power for the Secretary of State to make regulations providing that a person, for example browser or device suppliers, may not supply Information technology (IT) unless the IT meets requirements specified in the regulations.

Justification for the procedure

171. These regulations will be subject to the affirmative procedure and a consultation requirement. This is considered appropriate given the exercise of the power the first time would commence the principle requiring those subject to Regulation 6 of the PEC Regulations to respect consent/non-consent preferences expressed automatically through software or device settings. The power could also be used to alter the technologies that are recognised for the purposes of providing these automated signals.

Clause 87(1): Power to exclude use of electronic communication for the purposes of democratic engagement from direct marketing provision

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

172. Under the current PEC Regulations political parties cannot email/text prospective voters without prior consent or make phone calls to people who are registered with the telephone preference service or have previously asked not to be contacted. The government is of the view that this limits democratic engagement.

173. The government considers that democratic engagement is sufficiently important to dispense with the current PEC Regulations where political communication promotes aims/ideals for the purposes of democratic engagement.

174. Clause 87(1) confers powers on the Secretary of State to provide an exception from the direct marketing provision where “communications activity” is carried out solely for the purposes of democratic engagement by certain persons or organisations defined in the clause.

Justification for taking the power

175. The government recognises the importance of democratic engagement in a democracy and considers this power will help to facilitate democratic engagement. A number of safeguards have been inserted. The power would only apply in relation to communications sent by certain persons or organisations defined in the clause, for example, elected representatives, candidates seeking to become elected; registered political parties; or ‘permitted participants’ in connection with referendums as defined by relevant UK electoral legislation. The communications activity cannot be directed to individuals under the age of 14.

Justification for the procedure

176. These regulations will be subject to parliamentary scrutiny under the affirmative procedure. There is also a consultation requirement attached to it. Before making the regulations the Secretary of State is also required to consider the effect the regulations may

have on the privacy of individuals mindful that many people who responded to the consultation wanted electronic communications sent by political parties for the purposes of democratic engagement to be covered by the direct marketing rules in the PEC Regulations which would have required consent before engagement.

Clause 89(2): Power to amend fixed monetary penalty

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

177. This clause adds a new regulation 26A to the PEC Regulations, which introduces a new duty on a provider of a public electronic communication service or network to notify the Commissioner of any reasonable grounds the provider has for suspecting that a person is contravening or has contravened any of the direct marketing regulations in the course of using the service. The aim is to enable the Information Commission to better target its enforcement activity against nuisance marketing communications. The obligation to report is accompanied by a fixed penalty of £1,000 for failure to comply with any aspect of the reporting requirement (new regulation 26B).

178. The Bill will include a power for the Secretary of State to amend details of the reporting obligation, in particular those organisations subject to the obligation and the types of communication in scope, to ensure that it keeps pace with technological developments. The power will also enable the Secretary of State to increase the amount of the fixed penalty.

Justification for taking the power

179. The government considers this power necessary to ensure that the legislation remains in line with the current state of technology so as to enable the Information Commission to effectively target its enforcement actions in future, and to ensure that the amount of the fixed penalty remains appropriate and dissuasive.

Justification for the procedure

180. These regulations will be subject to the affirmative procedure. This is considered appropriate given the exercise of the power could alter the scope of the duty and the monetary value of the fixed penalty for failure to comply.

Clause 90(4): Power to amend fixed penalty amount

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

181. Under regulation 5A of the PEC Regulations, if a data breach occurs the “service provider” (a provider of a public electronic communications service) must notify the Information Commissioner within 24 hours, and also the user concerned if the breach is likely

to adversely affect their privacy without undue delay. Failure to do so incurs a fixed penalty of £1000 under regulation 5C of the PEC Regulations.

182. Similar requirements exist under articles 33 and 34 UK GDPR. Under article 33, a controller must communicate a personal data breach to the Information Commissioner within 72 hours unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Under article 34 the controller must communicate the breach to the data subject if there is a high risk to the rights and freedoms of natural persons without undue delay. Infringement of these obligations is subject to a penalty of the standard maximum level, which could be up to 2% of global annual turnover or £8.7 million (whichever is higher).

183. It has been decided to include a power in the PEC Regulations for the Secretary of State to change the fixed penalty amount set in regulation 5C of the PEC Regulations.

Justification for taking the power

184. The Bill will ensure that the enforcement regimes and penalty levels of the PEC Regulations with other data protection legislation create a more cohesive framework, including introducing the two-tier system of fines found in DPA 2018 and UK GDPR. The fixed penalty amount under regulation 5C of the PEC Regulations is a remaining notable disparity between the PEC Regulations and similar infringements under the UK GDPR.

185. However, the reporting requirements under the PEC Regulations and UK GDPR whilst similar are not identical. Articles 33 and 34 UK GDPR have a wider scope relating to controllers/ processors, whilst the PEC Regulations relate to public electronic communication service providers (which is mainly telecommunications and internet providers). Therefore it is not necessary to bring the PEC Regulations' penalty in line with UK GDPR right now as the government is satisfied that the £1000 fixed penalty is presently sufficient due to the Information Commissioner's effective relationship with the telecommunications sector. This current effectiveness may change in the future as technology and practices evolve and therefore the capability is needed to ensure the fixed penalty amount remains proportionate and dissuasive.

186. Further, as set out above the Bill will introduce a new duty in the PEC Regulations for service providers to report suspicious levels of activity. Infringement of this duty will incur a £1000 fixed penalty, with a power for the Secretary of State to amend this amount. Thus a power to amend the penalty amount under regulation 5C is required to maintain consistency within the PEC Regulations regime.

Justification for the procedure

187. Given the potentially significant increase in monetary penalties, parliamentary scrutiny under the affirmative procedure is considered appropriate. This will also cohere to the approach taken in the power for amending the fixed penalty for failure to report suspicious traffic, as set out above.

Clause 95(1): Power to remove the current recognition of trust services and trust service products which are qualified under equivalent EU law

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Negative procedure

Context and Purpose

188. This clause will allow for the amendment and revocation of article 24A of *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market* as amended upon EU exit by S.I. 2019/89 ("the UK eIDAS Regulation").

189. Under the UK eIDAS Regulation, trust service products provided by a *qualified* trust service provider established in the UK ("UK qualified trust service products") (including qualified electronic signatures, seals, timestamps, and registered delivery services) benefit from a presumption of legal integrity (for example Article 25(2) prescribes that a *qualified* electronic signature has the equivalent legal effect of a handwritten signature).

190. Article 24A of the eIDAS Regulation currently allows for elements of trust services (including trust service products) which are qualified under equivalent EU law, to be treated as *qualified* for the purposes of the UK eIDAS Regulation. This legal recognition under UK law is unilateral. Although trust service standards under EU law and UK law currently remain aligned post EU exit, trust services and products which are qualified for the purposes of the UK eIDAS Regulation only (i.e. provided by a qualified trust service provider established in the UK) are not legally recognised under equivalent EU law.

191. Article 24A requires that the UK continues to recognise EU qualified trust services and products on a unilateral basis, even if current aligned EU standards change and continuing to recognise new EU standards is not in the UK's national interests. In future the UK may wish to end the current recognition of EU qualified trust services, either because the EU changes its current trust service standards, and/or the UK qualified trust service market matures to an extent that it is no longer appropriate to unilaterally recognise EU qualified trust services.

Justification for taking the power

192. This clause allows for revocation of Article 24A at the point in future, once it is no longer appropriate from a policy perspective to recognise EU qualified trust services and products.

193. This power will also allow for amendment of Article 24A in order to wind down the current recognition of EU qualified trust services on a staggered basis (this might be necessary depending on potential future changes to EU trust service standards, and the comparative maturity of the UK qualified trust service market in future). For example, if standards for EU qualified signature and seal creation device do not change, whereas other EU trust service standards do, and such devices are still heavily relied upon by UK qualified trust service providers, this power could be exercised to amend Article 24A in order to only allow for the continued recognition of electronic signature and seal creation devices, which are qualified under EU law.

194. A staggered winding down of Article 24A is not possible to achieve, otherwise than through delegated legislation, whilst the final details of the right staggered approach (if necessary) are currently unknown and subject to future changes in EU trust service standards.

195. As well as the revocation and amendment of Article 24A, at the same time as ending the recognition of EU qualified trust services and products, this power will also allow for the revocation (and amendment) of other articles of the UK eIDAS Regulation and associated Implementing Decision (EU) 2015/1506 (which from a policy perspective are contingent upon recognising EU qualified trust services and products). This includes (amongst others) the

power to revoke the recognition of EU conformity assessment bodies under new Article 24B, and the power to remove references to a "trust service provider established in the EU".

Justification for the procedure

196. Although this power allows for amendment of the UK eIDAS Regulation (which is classed as retained direct principal EU legislation and so is treated in a similar way to primary legislation) it is appropriate that this power is subject to negative rather than affirmative procedure. This is on the basis that the power is not capable of altering the original policy underlying the UK eIDAS Regulation (standards and regulatory requirements for trust services within the UK) but instead is primarily limited to revoking provisions and removing related references, which were only necessary to insert within the UK eIDAS Regulation upon EU exit to ensure that the qualified trust service market within the UK could continue to operate.

197. So far as the power goes beyond the revocation of provisions and removal of references, in allowing for the amendment of Article 24A, this is to wind down the provision only, and is not capable of altering the fundamental policy behind Article 24A (recognition of EU trust services). Nor does the power to amend Article 24A allow for a widening of the scope of the provision, as there is no power to add an assumption to Article 24A(2) in order to recognise any element of EU qualified trust services which is not recognised currently.

Clause 96(2): Power to specify that certain overseas trust service products shall be treated as equivalent to qualified trust service products under the UK eIDAS Regulation (New Article 45A(1) of the UK eIDAS Regulation)

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Negative Procedure

Context and Purpose

198. This clause will insert new Article 45A into the UK eIDAS Regulation, in order to allow the Secretary of State by regulations to specify that certain trust service products (electronic signatures, seals, time stamps and registered delivery services) provided by a trust service provider established in a country or territory outside the UK, shall benefit from the same legal presumption of integrity and accuracy of data, which respective UK qualified trust service products benefit from under the UK eIDAS Regulation.

199. The purpose behind new Article 45A is to allow for the international interoperability of trust service products (in terms of their legal effect). In particular, by allowing the UK to make required changes to domestic law where UK qualified trust service products currently have a specified legal effect, in order to extend that effect to specified overseas trust service products. This will allow for international mutual recognition agreements, where it is agreed on a mutual basis that UK trust service products and their overseas equivalents shall have an equal legal effect.

Justification for taking the power

200. At this stage, recognising specified overseas trust service products on the face of the Bill would be premature. This is given that there are not yet any mutual recognition agreements in place with other countries allowing for the interoperability of trust service products.

201. A delegated power is therefore necessary in order to achieve recognition of specified overseas trust service products, at a point in future once it is appropriate to do so, either in order to give effect to a mutual recognition agreement concerning the interoperability of trust service products, or as part of wider trade negotiations, where the UK wishes to allow for the interoperability of trust service products.

202. Under new Article 45A(3) the Secretary of State may not make regulations specifying that a certain overseas trust service product shall be treated as legally equivalent to a comparable UK qualified trust service product, unless satisfied that the reliability of an overseas trust service product is at least equivalent to the reliability of the comparable UK qualified trust service product.

203. Recognising specified overseas trust service products through a delegated assessment of equivalent reliability, provides the scope to respond to future technological advances or changes to standards, which mean that further and new elements of overseas trust service frameworks will be relevant to consider in ensuring equivalent reliability of end trust service products.

204. The alternative approach of allowing for the recognition of certain overseas trust service products on the basis that rigid standards set within primary legislation are met (likely modelled around the UK's current trust service framework) would be at risk of redundancy, where overseas trust service frameworks advance over time, or differ from the UK's framework.

Justification for the procedure

205. This power is subject to negative procedure and a requirement under new Article 45C(1) for the Secretary of State to consult the UK's supervisory body for trust services (currently the Information Commissioner) before making regulations. Additional parliamentary scrutiny under the affirmative procedure, is not considered to be necessary for the reasons outlined below.

206. The exercise of this delegated power is subject to appropriate safeguards, including the requirement under Article 45A(3) that the Secretary of State must be satisfied that specified overseas trust service products are at least equivalent to the reliability of their counterparts under the UK eIDAS Regulation. There is also an additional constraint on the exercise of this power under Article 45A(4), that when making regulations the Secretary of State must have regard to (among other things) the relevant overseas law concerning the type of trust service product to be recognised.

207. Regulations made under Article 45A are then able to include conditions upon which the legal recognition of specified overseas trust service products is contingent, including conditions as to meeting specific requirements within overseas law, or meeting specific technical or regulatory standards.

208. The assessment of whether certain overseas trust service products are at least equivalent in terms of their reliability to comparable UK qualified trust service products will be technical and will require expertise of the UK qualified trust service industry. Through the consultation requirement under Article 45C(1), the Information Commissioner as the supervisory body for trust services with its technical and industry expertise, will therefore be best placed in order to assist with, and scrutinise, the Secretary of State's assessment as to whether overseas trust service products should be recognised.

209. Detailed and technical assessment of the factors as to whether an overseas trust service product offers equivalent reliability, would also form part of the negotiation process for agreeing any mutual recognition agreement giving rise to the need to exercise this delegated power.

Clause 96(2): Power to specify that certain overseas electronic signatures and seals shall be treated as equivalent for the use of online public services, to their counterparts under Articles 27(1) and (2), and 37(1) and (2) of the UK eIDAS Regulation (new Article 45B(1) and 45B(2) of the UK eIDAS Regulation)

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Negative Procedure

Context and Purpose

210. Existing Articles 27(1) and 37(1) of the UK eIDAS Regulation (provide respectively for electronic signatures and seals) that public sector bodies must recognise electronic signatures and seals which meet advanced standards, and additional technical standards under Implementing Decision 2015/1506 (retained EU law), where those public sector bodies require an advanced signature or seal for the use of an online public service.

211. Existing Articles 27(2) and 37(2) prescribe the same, but in respect of a requirement to accept, advanced electronic signatures and seals based on a qualified certificate (or qualified signatures and seals) which meet additional technical standards within Implementing Decision 2015/1506, where those public sector bodies require an advanced signature or seal based on a qualified certificate for the use of an online public service.

212. This clause will insert new Article 45B(1) into the UK eIDAS Regulation, in order to allow the Secretary of State by regulations to specify that certain electronic signatures provided by overseas trust service providers shall be treated for the purposes of Articles 27(1) or 27(2) respectively, as equivalent to advanced signatures which comply with Implementing Decision 2015/1506, or as equivalent to, advanced signatures based on qualified certificates (or qualifying signatures) which comply with Implementing Decision 2015/1506.

213. This clause will also insert new Article 45B(2) into the UK eIDAS Regulation, in order to allow the Secretary of State by regulations to specify that certain electronic seals provided by overseas trust service providers shall be treated for the purposes of Article 37(1) or 37(2) respectively, as equivalent to advanced seals with comply with Implementing Decision 2015/1506, or as equivalent to, advanced seals based on a qualified certificate (or qualifying seals) which comply with Implementing Decision 2015/1506.

214. The purpose behind new Article 45B(1) and (2) (as with Article 45A) is to allow for the international interoperability of trust service products (in terms of their legal effect). In particular, by allowing the UK to make required changes to domestic law so that specified overseas electronic signatures and seals are accepted (on an equal basis to their counterparts under the UK eIDAS Regulation) for the purposes of accessing online public services. This will allow for international mutual recognition agreements, where it is agreed on a mutual basis that UK trust service products, and their overseas equivalents shall have an equal legal effect.

Justification for taking the power

215. At this stage, recognising specified overseas electronic seals and signatures (in the context of use within online public services) on the face of the Bill would be premature. This is given that there are not yet any mutual recognition agreements in place with other countries allowing for the interoperability of trust service products.

216. A delegated power is therefore necessary in order to achieve recognition of specified overseas electronic seals and signatures (in the context of use within online public services) at a point in future once it is appropriate to do so, either in order to give effect to a mutual recognition agreement concerning the interoperability of trust service products, or as part of wider trade negotiations, where the UK wishes to allow for the interoperability of trust service products.

217. Under new Article 45B(4) the Secretary of State may not make regulations specifying that certain overseas electronic signatures or seals shall be accepted for the purposes of accessing online public services on an equal basis to their counterparts under the UK eIDAS Regulation, unless satisfied that the reliability of certain overseas electronic signatures or seals is at least equivalent to the reliability of their respective counterparts under Article 27(1), 27(2), 37(1), or 37(2) of the UK eIDAS Regulation.

218. Recognising specified overseas electronic signatures and seals through a delegated assessment of equivalent reliability, provides the scope to respond to future technological advances or changes to standards which mean that further and new elements of overseas trust service frameworks will be relevant to consider in ensuring equivalent reliability.

219. The alternative approach of allowing for the recognition of certain overseas electronic signatures and seals on the basis that rigid standards set within primary legislation are met (likely modelled around the UK's current trust service framework) would be at risk of redundancy, where overseas trust service frameworks advance over time, or differ from the UK's framework.

Justification for the procedure

220. This power is subject to negative procedure and a requirement under new Article 45C(1) for the Secretary of State to consult the UK's supervisory body for trust services (currently the Information Commissioner) before making regulations. Additional parliamentary scrutiny under the affirmative procedure, is not considered to be necessary for the reasons outlined below.

221. The exercise of this delegated power is subject to appropriate safeguards, including the requirement under Article 45B(4) that the Secretary of State must be satisfied that specified overseas electronic signatures and seals are at least equivalent to the reliability of their counterparts under the UK eIDAS Regulation. There is also an additional constraint on the exercise of this power under Article 45B(5), that when making regulations, the Secretary of State must have regard to (among other things) the relevant overseas law concerning the type of electronic signature or seal to be recognised.

222. Regulations made under Article 45B are then able to include conditions upon which the legal recognition of specified overseas signatures or seals is contingent, including conditions as to meeting specific requirements within overseas law, or meeting specific technical or regulatory standards.

223. The assessment of whether certain overseas signatures and seals are at least equivalent in terms of their reliability to their counterparts under the UK eIDAS Regulation will be technical and will require expertise of the UK trust service industry. Through the consultation requirement under Article 45C(1), the Information Commissioner as the supervisory body for trust services with its technical and industry expertise, will therefore be best placed in order to assist with, and scrutinise, the Secretary of State's assessment as to whether certain overseas electronics signatures or seals should be recognised.

224. Detailed and technical assessment of the factors feeding into whether a type of overseas electronic signature or seal offers equivalent reliability, would also form part of the negotiation process for agreeing any mutual recognition agreement giving rise to the need to exercise this delegated power.

Clause 97(3) & (5): Power to designate overseas authorities with which the Information Commissioner can share information, give assistance, or otherwise cooperate with

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Negative Procedure

Context and Purpose

225. Existing Article 24A of the UK eIDAS Regulation allows for the unilateral legal recognition within domestic law of trust service products which are qualified under equivalent EU law. Linked to this recognition, existing Article 18(1) of the UK eIDAS Regulation allows the Information Commissioner as the UK's supervisory body for trust services to give information and assistance to, and otherwise cooperate with a public authority in the EU, if the Information Commissioner considers that to do so would be in the interests of effective regulation or supervision of trust services.

226. Once the current unilateral recognition of trust service products which are qualified under equivalent EU law ends (through exercise of the delegated power under clause 89) it will no longer be necessary for the Information Commissioner to give information and assistance to, and otherwise cooperate with a public authority in the EU specifically.

227. Instead, once specified overseas trust service products are given a legal effect within domestic law, in the interests of effective regulation and supervision of trust services, it will be helpful for the Information Commissioner to retain the power to give information and assistance to or otherwise cooperate with another supervisory or regulatory body for trust services, but in respect of overseas supervisory and regulatory bodies more widely.

228. Accordingly, this clause amends Article 18(1) of the UK eIDAS Regulation, to include a power for the Information Commissioner to share information with, give assistance to, or otherwise cooperate with a *designated* overseas authority, instead of a public authority in the EU. Article 18(3) then contains a power for the Secretary of State by regulations to designate certain overseas regulatory or supervisory bodies for trust services, for the purposes of Article 18(1).

Justification for taking the power

229. At this stage, recognising certain overseas regulatory or supervisory bodies for trust services with which the Information Commissioner may give information and assistance to, or otherwise cooperate with, would be premature. This is given that overseas trust service products are not yet recognised through either mutual recognition agreements with other countries or within domestic law, and so information sharing and cooperation between the Information Commissioner and overseas supervisory and regulatory bodies, is not yet required.

230. A delegated power can be exercised on multiple occasions, where necessary, each time a mutual recognition agreement is entered into with another country and specified overseas trust service products are subsequently recognised within domestic law through the exercise of the separate new regulation making powers under Articles 45A and 45B. In contrast to the alternative of recognising relevant overseas regulatory or supervisory bodies in future within primary legislation, a delegated power will allow for information sharing and cooperation between the Information Commissioner and relevant overseas regulatory and supervisory bodies to align with the recognition of specific overseas trust services more widely. ,

Justification for the procedure

231. This power is subject to negative procedure and a requirement under new Article 18(4) for the Secretary of State to consult the Information Commissioner, as the UK's supervisory body for trust services before making regulations. Additional parliamentary scrutiny under the affirmative procedure, is not considered to be necessary, in part given the scope of the power to designate an *overseas authority* (which is defined as a person, or description of person, with functions relating to the regulation or supervision of trust services outside the UK) is relatively narrow.

232. Once an overseas authority has been designated within regulations, there is also an additional safeguard, in that the Information Commissioner in order to exercise its power under Article 18(1) must consider that giving information and assistance to, or cooperating with a designated overseas authority is in the interests of effective regulation or supervision of trust services. This means that the additional requirement for the Secretary of State to consult with the Information Commissioner before making regulations, should prevent an overseas authority being designated, where the Information Commissioner considers that it would not be able to exercise its power under Article 18(1) in respect of such an authority, in the interests of effective regulation or supervision of trust services.

233. In practice therefore, the exercise of the power to make regulations under Article 18(3) should be limited to the designation of overseas authorities which are responsible for the regulation or supervision of trust service products which are recognised by the UK, as these will be the overseas authorities to which giving information and assistance to and cooperating with, will be in the interests of effective regulation or supervision of trust services.

Clause 98: Power to disclose information to improve public service delivery to undertakings

Power conferred on: The appropriate national authority

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

234. This clause extends section 35 of the Digital Economy Act 2017 to allow information sharing to improve public service delivery to businesses. Currently, information may only be shared between specified public bodies for specific purposes related to public service delivery aimed at improving the well-being of individuals or households.

235. Section 35 of the Digital Economy Act 2017 ('DEA') contains delegated powers to (i) specify data sharing objectives, and (ii) specify public authorities that can share data for a specified objective by amending Schedule 4 to the DEA (a Henry VIII power). These powers are subject to the affirmative procedure and, under section 44(4) DEA, a duty to consult various bodies including the Information Commissioner, the Commissioners for Her Majesty's Revenue and Customs, appropriate national authorities and other persons considered appropriate.

236. The DEA allows the "appropriate national authority" to make regulations to add "specified persons" and "specified objectives". The "appropriate national authority", as defined in sections 44 and 45 of the DEA is the Secretary of State or Minister for the Cabinet Office, Scottish Ministers, Welsh Ministers or The Department of Finance in Northern Ireland.

237. This clause will extend the section 35 public delivery power to include businesses but will not change the robust safeguards in place around the use of section 35 powers.

238. Section 35 is a permissive gateway, which means it is at the discretion of the specified persons whether or not they choose to disclose information under the power.

239. The use of the information sharing power is underpinned by the statutory Code of Practice issued under section 43 of the DEA which contains guidance setting out best practice and the procedures and practices to be followed by specified persons.

Justification for taking the power

240. The specified objectives are set out in secondary legislation rather than primary legislation as the objectives for which information may be disclosed will need to be added to and amended to allow the power to keep pace with emerging social and economic needs, as well as the use of new streams of information to address them.

241. The specified persons are set out in secondary legislation rather than primary legislation as the list needs to be regularly updated to ensure that changing data sharing requirements can be enabled as further use cases emerge. The list may also need to be

updated to remove specified persons in accordance with section 35(6)(b) which provides a sanction for non-compliance with the Code of Practice.

242. Given the relative breadth of the power to share information under section 35 it is considered important that there be tightly controlled limits on the delegated power to specify persons, in particular it is recognised that there must be limits around the nature of the bodies that could be included in these lists. Therefore, there are a number of constraints on this delegated power.

243. To be a specified person the person must be a public authority or a person providing services to a public authority (Schedule 4, paragraph 28). In making regulations under section 35 the appropriate national authority must have regard to the systems and procedures the person has in place to ensure the secure handling of information by that person (section 35 (6)(a)). This is to ensure as far as possible that the integrity of the information shared is maintained.

244. To be a specified objective under section 35(7)-(12), an objective must meet three conditions set out on the face of the legislation. The first is that the objective has as its purpose a) the improvement or targeting of a public service provided to individuals or households, or b) the facilitation of the provision of a benefit (whether or not financial) to individuals or households (section 35 (9)). The second is that the objective has as its purpose the improvement of the well-being of individuals or households (section 35(10)). The third is that the objective has as its purpose the supporting of a) the delivery of a specified person's functions, or b) the administration, monitoring or enforcement of a specified person's functions (section 35(12)). This clause will amend these conditions to include services for businesses, but the essential framework and safeguards remain.

245. When it was introduced, the section 35 delegated powers regime was developed in line with DPRRC's recommendations (13th Report of Session 2016–17, published 19 January 2017 and the government's response in the 18th Report of Session 2016–17 published 23 February 2017). This clause will operate within that same regime.

246. Any data sharing done under section 35 must be carried out in accordance with the requirements of the DPA 2018 and UK GDPR.

Justification for the procedure

247. As this clause provides the appropriate national authority with a delegated power to specify objectives and bodies which bodies may share information under each objective, it is considered appropriate that the use of the power is debated and subject to more intensive scrutiny by Parliament via the affirmative procedure as well as consulting the Information Commissioner, other appropriate national authorities, the Commissioners for Her Majesty's Revenue and Customs and such other persons as the appropriate national authority thinks appropriate.

Clause 99(1): Power to implement international agreements on sharing information for law enforcement purposes

Power conferred on: The appropriate national authority

Power exercised by: Regulations

Parliamentary Procedure: Negative procedure

Context and Purpose

248. The Secretary of State has prerogative powers to enter into international agreements (whether by way of treaties or memoranda of understanding) with third party nations governing the sharing of data for law enforcement ("LE") purposes.

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

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

251. The "appropriate national authority", is defined in clause 100 as, the Secretary of State, Scottish Ministers, and Welsh Ministers, are also appropriate national authorities in relation to regulations under clause 99 which would be within the legislative competence of the Scottish Parliament or Senedd Cymru, respectively. Whilst international relations are a reserved matter, the domestic implementation of such agreements is devolved, and law enforcement is a devolved matter to varying extents in each devolved administration. A concurrent power to make regulations has not been included for Northern Ireland, as presently there is not a functioning Executive, and the Assembly is not sitting. It has been agreed the Secretary of State will make regulations relating to Northern Ireland.

Justification for taking the power

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

253. Regulations made under this power will set out the technical details needed to implement an international LE data sharing agreement (e.g., the IT software to be used, the timescales by which data should be provided, etc). Such regulations may also include operational details. Regulations are desirable to provide clarity for frontline officers and international partners.

Justification for the procedure

254. In the circumstances, the negative procedure is appropriate. The technical detail, including IT specification, flowing from the overarching agreements does not require the maximum level of scrutiny of Parliament. The regulations will mostly be for the benefit of frontline officers and the relevant international partners, providing them with clarity and a framework to follow when sharing data. Parliament would likely be neutral about the content of the detailed technical specifications.

255. It would not be a proportionate use of Parliament's time to debate the IT processing or other details flowing from any main agreements.

256. If Parliament were to scrutinise the detail of the implementation SIs, it would not amount to scrutiny of the overarching agreements. In any event, where an overarching agreement is made by way of a treaty, Parliament may scrutinise that treaty pursuant to the Constitutional Reform and Governance Act 2010.

Clause 103(2): Power to set out requirements in relation to signing a birth or death register

Power conferred on: The Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

257. This clause inserts a new section 38B into the Births and Deaths Registration Act 1953 (BDRA), enabling the Secretary of State to make regulations in relation to the requirement to sign a birth or death register where the register is required to be kept otherwise than in hard copy form. The regulations may provide that a person's duty under the BDRA to sign the birth or death register is to have effect as a duty to comply with alternative, specified requirements, and a person who complies with those requirements is to be treated as having signed the register and to have done so in the presence of the registrar. Under new section 38B(2) of BDRA, the regulations may (among other things) require a person to sign something other than the birth or death register and/or provide evidence of identity.

Justification for taking the power

258. The main purpose of the "registers of births and deaths" clauses is to remove the requirement for births and deaths registers to be held in hard copy form, thus enabling the introduction of an electronic register. A number of provisions in the BDRA require an informant to sign the register in the presence of the registrar when registering a birth or a death. The power conferred by this clause would enable alternative requirements to be set, so that the informant does not need to sign the register in the presence of the registrar once the register is no longer maintained in hard copy form. It is considered appropriate for the detail of the alternative requirements to be contained in regulations, as they will set out detailed administrative procedure and may require adjustment over time.

Justification for the procedure

259. Regulations made under this power will, pursuant to new section 39A(6), be subject to the affirmative resolution procedure requiring a draft to be laid before and approved by a resolution of both Houses of Parliament. We propose that this is the appropriate procedure for these regulations, allowing Parliament to consider the alternative requirements that will replace signing the register and ensure they are robust.

Clause 113(5): Amendment of duty of board to issue guidance

Power conferred on: Board established under section 63AB of the Police and Criminal Evidence Act 1984

Power exercised by: Code of Practice

Parliamentary Procedure: None

Context and Purpose

260. The amendments made by the Protection of Freedoms Act 2012 to the Police and Criminal Evidence Act 1984 established a DNA Database Strategy Board to oversee the operation of the National DNA Database. The amendments required that Board to issue guidance about the destruction of DNA profiles and also required the chief officer of a police force in England and Wales to act in accordance with the guidance.

261. Clause 113 amends the existing requirement in subsection (2) of section 63AB of the Police and Criminal Evidence Act 1984 for the board to issue guidance to a requirement to issue one or more codes of practice about the erasure of personal data from a database listed in subsection (1), about the destruction of DNA profiles and the destruction of other material which biometric data contained in a database listed in subsection (1) is derived.

Justification for taking the power

262. Clause 113 will require the Board to oversee the national fingerprint database and enable it to oversee other biometric databases as required in the future. In exercising this function the Board needs to set out the policy and procedures police forces must comply with in order to meet the requirements of relevant data protection legislation, including how biometric data should be stored, accessed and deleted on the database. This ensures consistency in procedures across policing. The clause will require the Board to issue codes of practice for this purpose,

Justification for the procedure

263. The codes of practice will provide technical guidance for policing on how the relevant legislation applies to a specific database, supporting chief officers to comply with the requirements of the Police and Criminal Evidence Act 1984 and the data protection legislation, and the operational procedures associated with the destruction of physical material and erasure of personal data. As the code of practices are enabling compliance with an existing statutory framework it is not considered necessary for this to be subject to parliamentary scrutiny.

Clause 113(11): Power to extend the remit of the Board over biometrics databases

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

264. The Protection of Freedoms Act 2012 (PoFA) introduced a new requirement for the Secretary of State to make arrangements for a National DNA Database Strategy Board to oversee the operation of the National DNA Database (section 63AB of the Police and Criminal Evidence Act 1984). PoFA amended the Police and Criminal Evidence Act 1984 to require any DNA profile which is retained under any of the powers in section 63E to 63L of that Act to be recorded on the National DNA Database for use by police forces in England and Wales (section 63AA).

265. Clause 113 amends section 63AB of PACE to require the Board to oversee the database of fingerprints which have been taken from any person under a power conferred by Part 5 of PACE or taken by the police in connection with the investigation of an offence. The clause also changes the name of the Board to the Forensic Information Database Strategy Board.

266. The clause also amends section 63AB to include in subsection (10) a new power for the Secretary of State by regulations to change the databases which the Board is required to oversee to add another database consisting entirely or mainly of biometric data or genetic data which is used for policing purposes. There is an associated power to rename the Board. There is also a power to remove a database. The Secretary of State may also require or authorise the Board to issue a code of practice or guidance. There is a consequential power enabling the regulations to amend section 63AB, or make different provision for different purposes as well as to make any consequential, transitional, transitory or saving provisions in respect of the removal of a database or the inclusion of a new database in the databases overseen by the Board.

267. Regulations made under this power may amend provisions of primary legislation (subsection (11)(a)), and it is therefore a Henry VIII power.

Justification for taking the power

268. There is a need for flexibility in the databases which the Board oversees given the pace of technological change and requirement for consistent oversight. This will enable a new database of biometric data used for policing purposes to be added to the legislation within the existing framework, or where a database is no longer used, it can be removed. While DNA and fingerprints are well established, biometrics is an area of rapid technological development, including for example iris, face, voice and keystroke patterns. The government is looking to simplify and provide more consistency in the oversight of the police use of biometrics. If and when a new biometric database used for policing purposes reaches a similar level of maturity to DNA and fingerprints, there are likely to be benefits in terms of consistency to bring it within the oversight of the Board, as similar considerations are likely to apply. The delegated power would enable a new database to be added to the existing legislative framework.

Justification for the procedure

269. As the regulations will enable primary legislation to be amended it is appropriate that the regulations should be made under the affirmative procedure.

Clause 114(1): Power to make consequential amendments

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure where regulations amend primary legislation; otherwise negative procedure

Context and Purpose

270. This clause provides the Secretary of State with the power to make provision that is consequential on this Bill.

271. Regulations made under this power may amend or repeal or revoke provisions of primary legislation (subsection (2)(c)), and it is therefore a Henry VIII power.

272. Regulations making provision consequential on the abolition of the Information Commissioner, and his replacement by the new Information Commission, are permitted to amend primary legislation whenever passed or made, including the Bill. But regulations making provision consequential on other provisions of the Bill may only amend primary legislation passed or made before the end of the Session in which the Bill is passed.

Justification for taking the power

273. The power conferred by this clause is wide but is limited by the fact that any amendments made under it must be genuinely consequential on provisions in the Bill. It will be necessary to use this power to amend the Bill itself in order to ensure that the provisions in the Bill operate correctly with respect to the new regulator.

274. The Bill makes numerous amendments to existing legislation, in particular the UK GDPR and DPA 2018, which may require updates to any relevant cross-references in other legislation to provide legal certainty. It is not possible to establish in advance all consequential amendments that may be required. The power will therefore be used to make any relevant

provision upon the commencement of the substantive provisions of this Bill. There are numerous precedents for such a power, for example, section 211 DPA 2018.

Justification for the procedure

275. If regulations under this clause do not repeal, revoke or otherwise amend primary legislation they will be subject to the negative resolution procedure (by virtue of subsection (5)). If regulations under this clause amend or repeal provision in primary legislation (including this Bill) they will be subject to the affirmative resolution procedure (by virtue of subsection (4)) as befitting a Henry VIII power of this type. It is considered that this provides the appropriate level of parliamentary scrutiny for the powers conferred by this clause.

Clause 119(1): Power to commence provisions

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: None

Context and Purpose

276. This clause deals with the commencement of the provisions of the Bill. The provisions listed in subsection (2) will come into force when the Act is passed. The remaining provisions will come into force on a day appointed by the Secretary of State through regulations and these can be different days for different provisions.

Justification for taking the power

277. Leaving provisions in the Bill to be brought into force by regulations will enable the government to commence the provisions of the Bill at the appropriate time, having regard to the need to make any necessary secondary legislation, issue guidance, and enable businesses and other organisations adequate time to undertake appropriate training and put the necessary systems and procedures in place, as the case may be.

Justification for the procedure

278. As usual with commencement powers, regulations made under this clause are not subject to any parliamentary procedure. The principle of the provisions to be commenced will already have been considered by Parliament during the passage of the Bill. Commencement by regulations enables the provisions to be brought into force at a convenient time.

Clause 120(1): Power to make transitional provision

Power conferred on: The Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Negative procedure for amendments to Schedule 21 DPA 2018 and Part 2 of Schedule 7 to this Bill, otherwise none

Context and Purpose

279. This clause confers a power on the Secretary of State to make regulations making transitional, transitory, or saving provision in connection with the coming into force of any provision of the Bill.

280. This power enables the Secretary of State to amend Schedule 21 to DPA 2018 (Further transitional provision etc) or Part 2 of Schedule 7 to this Bill (Consequential and transitional provision) and is therefore a Henry VIII power. Schedule 21 was added to DPA 2018 by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and includes transitional provisions designed to ensure that established data flows from the UK to third countries could continue after the UK left the EU. Part 2 of Schedule 7 to this Bill includes transitional provisions designed to ensure a smooth transition to new rules on international transfers introduced by this Bill.

Justification for taking the power

281. This standard power ensures that the Secretary of State can provide a smooth commencement of new legislation and transition between existing legislation (principally DPA 2018) and the Bill, without creating any undue difficulty or unfairness in making these changes. There are numerous precedents for such a power, including in section 213 DPA 2018.

282. If the international transfer rules (currently in Parts 2 & 3 of the DPA 2018 and Chapter V of the UK GDPR) are amended during the Bill's progress through Parliament that might necessitate changes to the transitional provisions in Part 2 of Schedule 7 to the Bill. Ensuring that such provision is as effective as possible for businesses and other organisations affected may require changes to related transitional provisions in Schedule 21 to DPA 2018. For this reason the power enables changes to be made to these provisions, but is limited to these provisions and does not extend to other transitional provisions such as in Schedule 20 to DPA 2018.

Justification for the procedure

283. Exercise of this power is not subject to any parliamentary procedure, except when it is used to amend primary legislation.

284. Such a power is commonly included as part of a bill's power to make commencement regulations and such regulations are not usually subject to any parliamentary procedure on the grounds that Parliament has already approved the principle of the provisions in the Bill by enacting them. Although drafted as a free-standing power on this occasion, the same principle applies.

285. Where the power is exercised to amend primary legislation it is appropriate to subject it to parliamentary procedure. Whilst powers to amend primary legislation would usually be subject to the affirmative procedure, the negative procedure is appropriate in this case because of the nature of the power as described above. This is consistent with the approach taken in section 213 DPA 2018.

Schedule 5, paragraph 4: Power to approve transfers by regulations

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Negative procedure

Context and Purpose

286. The UK GDPR currently provides for three mechanisms under which personal data can be transferred overseas. The first of these mechanisms is where the Secretary of State has made regulations specifying that the data protection standards of the jurisdiction provide

an adequate level of protection. Such regulations effectively 'whitelist' a country for the purposes of personal data transfers.

287. This regulation-making power already exists in the current legislation in section 17A DPA 2018, read alongside Chapter V of the UK GDPR. The Bill will amend the provisions associated with the power to create a clearer regime for approving transfers to other countries, to reflect the way in which the UK approaches such determinations. The regulation-making power and associated provisions will be moved into the UK GDPR.

Justification for taking the power

288. This restates a Secretary of State power that already exists in the current legislation. There will be some changes to the test which has to be met in order for the Secretary of State to approve a country to receive unrestricted transfers of personal data to which the UK GDPR applies, and other aspects of the associated provisions, but the underlying effect of the power will remain the same.

289. Given that countries' data protection regimes evolve frequently, and given the length of time it takes to conduct an assessment of a country's data protection regime, it would be impractical and lead to unnecessary delays if new primary legislation were required each time it was considered appropriate to allow unrestricted transfers of personal data to a new country. Granting the power to the Secretary of State to approve countries which meet the standards set out in primary legislation will mean that countries can be approved more quickly, benefiting UK organisations and individuals. Transfers under this mechanism lead to significant reductions in barriers that businesses, researchers and government organisations face when transferring personal data overseas.

290. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see new Article 91A UK GDPR added by clause 46 of this Bill).

Justification for the procedure

291. The existing regulation making power under section 17A DPA 2018 is subject to the negative resolution procedure and the power as restated in paragraph 4 of Schedule 5 will be subject to the same procedure. Negative resolution is considered sufficient scrutiny given the clear parameters, set out in primary legislation, within which this power can be used.

Schedule 5, paragraph 8: Power to specify standard contractual clauses by regulations

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Negative procedure

Context and Purpose

292. The UK GDPR currently provides for three mechanisms under which personal data can be transferred overseas. The first of these mechanisms is set out above. The second of these mechanisms allows personal data to be transferred, in the absence of adequacy regulations, where appropriate safeguards are in place. Appropriate safeguards may be provided, among other methods, by the use of standard contractual clauses which the Secretary of State has laid by way of regulations.

293. This regulation-making power already exists in the current legislation in section 17C DPA 2018, read alongside Chapter V of the UK GDPR. The Bill will amend the provisions

associated with the power to create a clearer regime for transferring data subject to appropriate safeguards. The regulation-making power and associated provisions will be moved into the UK GDPR.

Justification for taking the power

294. This restates a Secretary of State power that already exists in current legislation.

295. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see new Article 91A UK GDPR added by clause 46 of this Bill).

Justification for the procedure

296. The existing regulation-making power in section 17C DPA 2018 is subject to the negative resolution procedure and the power as restated in paragraph 8 of Schedule 5 will be subject to the same procedure. Negative resolution is considered sufficient scrutiny given the clear parameters, set out in primary legislation, within which this power can be used.

Schedule 5, paragraph 8: Power to make provision about further safeguards by regulations

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

297. This provision will give the Secretary of State the power to recognise new mechanisms for transfers to complement those set out in Articles 46(2) and (3) of the UK GDPR. The Secretary of State will be empowered to recognise new mechanisms as being capable of providing 'appropriate safeguards' for transfer as referred to in Article 46(1). Any new transfer mechanism recognised by the Secretary of State under this power will need to be capable of providing the same standard of protection for data subjects as existing transfer mechanisms under Article 46.

Justification for taking the power

298. This power will support the UK government to adapt at pace to international developments in data protection law, as well as reflect the increasing importance of multilateral cooperation in maintaining global data flows while ensuring a high standard of data protection.

299. The power will complement and extend the Secretary of State's existing power under Article 46(2)(c) and section 17C DPA 2018 to specify standard data protection clauses. While some novel transfer mechanisms (such as the EU's new standard contractual clauses issued in accordance with Article 46(2)(c) of the EU GDPR) could be recognised under this existing power, there are other tools, such as those created under international privacy schemes, which would not fit into the bounds of Article 46(2)(c).

300. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see new Article 91A UK GDPR added by clause 46 of this Bill).

Justification for the procedure

301. The affirmative resolution procedure will maintain Parliamentary scrutiny over the process of designating transfer mechanisms as capable of providing the appropriate safeguards required by Article 46(1). Opening new routes for personal data flows overseas has the potential to have a substantial effect on data subjects and their rights, so it is appropriate that Parliament maintains scrutiny over this process. It is also a broader power than set out in section 17C DPA 2018, which empowers the Secretary of State to specify in regulations (subject to the negative resolution procedure) standard contractual clauses that the Secretary of State considers to provide appropriate safeguards. As such, and because regulations under this power have the potential to impact data subject rights in a broader manner, it is appropriate that its use is subject to the affirmative resolution procedure.

Schedule 5, paragraph 9(5): Power to specify where a transfer is taken to be necessary or not necessary for the public interest

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Made affirmative procedure where the Secretary of State has made an urgency statement in respect of them, otherwise the affirmative procedure

Context and Purpose

302. The UK GDPR currently provides for three mechanisms under which personal data can be transferred overseas. The first and second of these mechanisms are set out above. The third of these mechanisms allows personal data to be transferred using derogations if specific circumstances apply. One such situation includes where the transfer is necessary for important reasons of public interest which have been recognised in domestic law (whether by regulations or otherwise) ("the Article 49(1)(d) derogation").

303. A power already exists in section 18(1) DPA 2018 to specify by regulations circumstances in which a transfer is taken to be necessary for important reasons of public interest, and circumstances in which a transfer is not taken to be necessary for important reasons of public interest, for the purposes of the Article 49(1)(d) derogation.

304. The Bill moves the existing power in section 18(1) DPA 2018 into Article 49(4A), as part of the restructuring of the international transfers regime provisions in the UK GDPR and DPA 2018 so that all provisions relating to international transfers will be contained in Chapter V of the UK GDPR, for clarity and ease of reference. No changes are being made to the power itself.

Justification for taking the power

305. This restates a power of the Secretary of State which already exists in the current legislation. It is not possible for the UK government to identify and set out all current and future matters of public interest in the Bill - and should any need emerge in future, this power will give the Secretary of State the power to specify any such matters. This power will also give the Secretary of State the ability to stop or prevent improper uses of the Article 49(1)(d) derogation which are not in the public interest, which it is not possible to predict at this time. Although no such uses have been identified for inclusion in the Bill at this time, the power provides a valuable safeguard to help protect individuals' personal data.

306. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate, except where the Secretary of State has made an urgency statement (see new Article 91A UK GDPR added by clause 46 of this Bill).

Justification for the procedure

307. The existing regulation-making power in section 18(1) DPA 2018 is subject to the made affirmative resolution procedure where the Secretary of State has made an urgency statement in respect of them; otherwise it is subject to the affirmative resolution procedure. The power as restated in Article 49(4A) of the UK GDPR will be subject to the same procedure, which is considered appropriate as while Parliament should have the ability to approve matters designated as being necessary or not necessary for important reasons of public interest through the affirmative procedure, there may be circumstances in which action needs to be taken quickly to protect individuals' personal data - particularly in relation to specifying matters not in the public interest - so permitting the made affirmative procedure in urgent circumstances is appropriate.

Schedule 5, paragraph 10: Power to restrict transfers for the public interest

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Made affirmative procedure where the Secretary of State has made an urgency statement in respect of them, otherwise the affirmative procedure

Context and Purpose

308. Section 18(2) DPA 2018 currently confers on the Secretary of State a power to restrict the transfer of categories of personal data to a third country or international organisation, if the Secretary of State considers that such a restriction is necessary for important reasons of public interest. This power can only be exercised where there are no adequacy regulations in place permitting the transfers in question.

309. The Bill moves the existing power in section 18(2) DPA 2018 into new Article 49A, as part of the restructuring of the international transfers regime provisions in the UK GDPR and DPA 2018 so that all provisions relating to international transfers will be contained in Chapter V of the UK GDPR, for clarity and ease of reference. No changes are being made to the power itself.

Justification for taking the power

310. This restates a power of the Secretary of State which already exists in the current legislation. It provides a further safeguard to protect individual's personal data by preventing categories of personal data from being transferred to another country where the Secretary of State believes it is in the public interest to do so. There are no such situations which currently exist, but it is not possible to predict all of the possible future scenarios in which personal data may be at risk, and so it is appropriate for the Secretary of State to be given the power to impose such restrictions.

311. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate, except where the Secretary of State has made an urgency statement (see new Article 91A UK GDPR added by clause 46 of this Bill).

Justification for the procedure

312. The existing regulation-making power in section 18(2) DPA 2018 is subject to the made affirmative resolution procedure where the Secretary of State has made an urgency statement in respect of them; otherwise it is subject to the affirmative resolution procedure.

The power as restated in new Article 49A of the UK GDPR will be subject to the same procedure, which is considered appropriate as while Parliament should have the ability to approve restrictions being imposed on the transfer of categories of personal data to another country, there may be circumstances in which action needs to be taken quickly to mitigate against risks to individuals' personal data which arise when they are transferred to other countries, so permitting the made affirmative procedure in urgent circumstances is appropriate.

Schedule 6, paragraph 4: Power to approve transfers by regulations

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Negative procedure

Context and Purpose

313. Chapter 5 of Part 3 of the DPA 2018 currently provides for three mechanisms under which personal data can be transferred overseas for law enforcement purposes. The first of these mechanisms is where the Secretary of State has made regulations specifying that the data protection standards of the jurisdiction provide an adequate level of protection. Such regulations reduce the barriers for sharing personal data with third countries and international organisations, helping to ensure such important data sharing can take place.

314. This regulation-making power already exists in the current legislation in section 74A DPA 2018. This Bill will amend the provisions associated with the power to create a clearer regime for approving transfers to other countries, to reflect the way in which the UK approaches such determinations. The changes being made to this power in Part 3 of the DPA 2018 mirror the changes being made to the equivalent power in the UK GDPR (paragraph 4 of Schedule 5) already detailed above.

Justification for taking the power

315. This restates a Secretary of State power that already exists in the current legislation. There will be some changes to the test which has to be met in order for the Secretary of State to approve a country for transfers of personal data to which Part 3 of the DPA 2018 applies, and other aspects of the associated provisions, but the underlying effect of the power will remain the same.

316. As already detailed for the equivalent change in the UK GDPR (paragraph 4 of Schedule 5), it would be impractical and lead to unnecessary delays if new primary legislation were required each time the Secretary of State assessed and considered it was appropriate to allow transfers of personal data to a new country. Allowing this to be done by regulations ensures the process can be done more quickly, which benefits competent authorities needing to share data for law enforcement purposes overseas, enabling them to share data with international partners.

317. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see section 182 DPA 2018).

Justification for the procedure

318. The existing regulation making power under section 74A DPA 2018 is subject to the negative resolution procedure and the power as restated in paragraph 4 of Schedule 6 will

be subject to the same procedure. Negative resolution is considered sufficient scrutiny given the clear parameters, set out in primary legislation, within which this power can be used.

Schedule 10, paragraph 1: Power to make provision about penalties

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Affirmative procedure

Context and Purpose

319. As part of the objective of aligning the PEC Regulations's enforcement regime with that of the DPA 2018, sections 157 and 159 DPA 2018 will be applied to the PEC Regulations. The applied version of section 157 DPA 2018 sets out the maximum penalty amounts that the Commissioner can impose on a person for infringement of the PEC Regulations. Just as there is under DPA 2018, there are two penalty maximums depending on the nature of the infringements: a higher maximum amount and a standard maximum amount. The higher maximum amount, in the case of "an undertaking", is £17.5 million or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, and in any other case the higher maximum amount is £17.5million. The standard maximum amount, in the case of "an undertaking", is £8.7 million or 2% of the undertaking's total annual worldwide turnover in the preceding financial year, and in any other case the higher maximum amount is £8.7 million.

320. Section 159 DPA 2018 enables the Secretary of State to make regulations which make further provision about administrative penalties and this section will be applied to the PEC Regulations. The provision which such regulations can make are:

a. whether a person is or is not "an undertaking";
b. how an undertaking's turnover is to be determined; and
c. whether a period is or is not a financial year.

321. As section 159 will now be applied to the PEC Regulations, this is effectively an extension of scope of the Secretary of State's powers.

Justification for taking the power

322. The provisions in the DPA 2018 as applied to the PEC Regulations provide for different maximum fines depending on whether the person on whom the fine is to be imposed is an "undertaking". Having established in the DPA 2018 (and on the face of the Bill for application to the PEC Regulations) a formula for calculating the maximum fine that may be imposed on an undertaking, it is appropriate to leave to regulations the secondary detail as to which legal persons are to be treated as being, or not being, an undertaking (which may range from commercial undertakings to different forms of public body), how to determine an undertaking's turnover (which may vary according to the nature of the undertaking) and how to define an undertaking's financial year.

323. These powers replicate those which already exist in the DPA 2018 and are required to ensure cohesion and consistency between the enforcement regimes of DPA 2018 and the PEC Regulations.

Justification for the procedure

324. These powers are subject to the affirmative procedure. This is considered appropriate given that, in particular, the definition of an undertaking will determine those organisations which are potentially subject to a higher maximum monetary penalty calculated by reference

to a percentage of their turnover. This is the procedure already decreed in section 159(3) DPA 2018.

Schedule 12, paragraph 3: Power to publish information standards

Power conferred on: Secretary of State

Power exercised by: Published standards

Parliamentary Procedure: None

Context and Purpose

325. Section 250 of the Health and Social Care Act 2012 (HASCA 2012), as amended by the Health and Care Act 2022, concerns information standards. These are standards in relation to the processing of information which may be prepared and published by the Secretary of State (in connection with the provision of health and adult social care) and NHS England (in connection with the provision of NHS services). Under section 250, as amended, information standards must be complied with.

326. This provision amends section 250 to make it clear that information standards published under that section can include standards relating to information technology or information technology services used to process information. It also extends the categories of persons to which information standards may be applied to include information technology providers i.e. persons involved in making available information technology, information technology services or a service which consists of processing information using information technology, for use in connection with the provision in, or in relation to, England of health or adult social care. Currently, under section 251(3) of the HASCA 2012, the Secretary of State or NHS England may adopt an information standard prepared or published by another person. The clause expands this to such information standards as they have effect from time to time, and enables provision to be made by reference to international agreements or other documents (including as they have effect from time to time).

327. The provision would also have the consequential effect of expanding the scope of regulation making powers and duties which apply in relation to section 250 under the HASCA 2012, namely:

a. a power for regulations to enable the Secretary of State or NHS England to waive compliance with information standards (section 250(6B)) which may limit the circumstances in which waivers may be granted, set out the procedure to be followed in connection with waivers, and require an information standard to include specified information about waivers (section 250(6C));

b. a duty to make regulations about the procedure to be followed in connection with the preparation and publication of information standards (section 251(1)(a));

c. a power for regulations to require an information standard to be reviewed periodically (section 251(1)(b));

d. a power for regulations to provide for financial penalties in respect of failure to comply with information standards (section 277E(1)(a)); or in respect of a requirement imposed under section 251ZA(1) to provide the Secretary of State with information for the purposes of monitoring compliance with information standards (section 277E(1)(b)); or in respect of the provision of false or misleading information (section 277E(1)(c)).

Justification for taking the power

328. The information standards to be applied in relation to information technology and information technology services will largely be of a technical nature (for example, interface specifications) and relate to matters such as design, quality, capabilities, arrangements for marketing and supply, functionality, connectivity, interoperability, portability and storage and security of information. These are matters of detail that are more appropriate for published, technical standards which are created and can be updated through a statutory procedure. The information technology landscape is an evolving one and could necessitate frequent changes to the standards imposed in order for them to be kept up to date. The delegated powers engaged by this clause will enable the government to keep pace with change and adapt the standards accordingly.

Justification for the procedure

329. Given that the information standards will largely be of a technical nature and reflect the current state of advancement in the field of information technology, and given that the clause extends the scope of existing legislation with respect to information standards, it is not considered necessary for such information standards to be subject to Parliamentary scrutiny when published. The regulation making powers and duties affected by these changes (including powers and duties to make provision about the procedure by which information standards are prepared and published and about financial penalties) will be subject to the affirmative Parliamentary procedure and this continues to represent the appropriate level of scrutiny.

Schedule 12, paragraph 8, new section 251ZD: Power to direct a public body or to make arrangements for a person prescribed by regulations to exercise functions relating to monitoring and requesting compliance

Power conferred on: Secretary of State

Power exercised by: Regulations and directions

Parliamentary Procedure: Negative procedure in relation to regulations; no procedure in relation to directions

Context and Purpose

330. New section 251ZD(1) enables the Secretary of State to direct a public body (person whose functions are of a public nature) to exercise the Secretary of the State's functions under section 251ZA of the HASCA 2012 (power to require information for the purposes of monitoring compliance with information standards) so far as they relate to information technology providers, and under section 251ZB (power to request information technology providers to comply with information standards). It also enables the Secretary of State to give directions about the exercise of those functions, including directions as to the processing of information obtained by exercising the functions. New section 251ZD(2) also enables the Secretary of State to make arrangements for a person prescribed by regulations to exercise those functions.

Justification for taking the power

331. The Secretary of State needs to have options for the exercise of the functions in operational terms, and to retain the discretion to delegate, or to not delegate, them to another person, to revoke a decision to delegate and to ensure that the most appropriate person exercises the functions, the identity of which may fluctuate over time. The power to direct a public body about the exercise of the functions in question is necessary in order to cover

matters such as how the functions are to be exercised. Thus, the directions would contain matters of administrative or operational detail which may need to be updated regularly. This would enable the Secretary of State to cater to changing circumstances.

Justification for the procedure

332. The regulations would relate to the identity of the person to whom the Secretary of State's functions are to be delegated and this may fluctuate over time. The negative procedure is considered to provide the appropriate level of scrutiny for this. In relation to directions, which would be required to be given in writing, the power would concern the question of whether an existing function should be exercised by a public authority rather than the substance of the functions. The authority would be bound by any constraints which apply in relation to the exercise of the functions. Given the administrative and operational nature of the directions, Parliamentary scrutiny is considered unnecessary.

Schedule 12, paragraph 8, new section 251ZE: Power to establish accreditation scheme

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Negative procedure

Context and Purpose

333. This provision would enable the Secretary of State, by regulations, to establish an accreditation scheme that might be run by a specified body. The scheme would relate to information technology or information technology services. Subsections (3) and (4) of inserted section 251ZE set out the potential scope of the regulations, for example they may require the operator to set accreditation criteria by reference to information standards or to provide for the review of decisions. The operator may also be required by the regulations to provide advice to applicants for accreditation. An accreditation scheme would be intended essentially to grant a quality mark to information technology and information technology services that meet specified criteria to enable information technology providers to demonstrate that that technology or those services meet the necessary quality standards. The operator of a scheme could be given power under the regulations to determine the accreditation criteria or be permitted to charge a reasonable fee in respect of an application for accreditation.

Justification for taking the power

334. The procedures for the operation of an accreditation scheme would be technical and require more detail to describe than would usually be included in primary legislation.

Justification for the procedure

335. The negative resolution procedure provides for the appropriate level of scrutiny for standard provisions of this kind. There is precedent for this in relation to regulations concerning accreditation schemes under section 267 of the HASCA 2012, which are similarly subject to the negative procedure.

Schedule 13, paragraph 2(3) of new Schedule 12A to the DPA 2018: Power to amend maximum number of members

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: Negative procedure

Context and Purpose

336. The purpose of this part of the legislation is to change the governance structure of the office of the Information Commissioner, formerly a corporation sole with all powers and responsibilities vested in the role of the Information Commissioner, creating instead a new statutory corporation with a new governance model to be known as the Information Commission which, in particular, provides that the current functions of the Information Commissioner are shared between the executive and non executive members of the board. In accordance with recent practice, the legislation expressly provides for a minimum and maximum number of board members. This provision gives the power to the Secretary of State to make regulations to alter the maximum number of members of the Commission set out in paragraph 2(2) of new Schedule 12A to the DPA 2018, and it is therefore a Henry VIII power. There is a relevant precedent for a power of this sort to be subject to the negative resolution procedure: see section 1(7) and (8) of the Office of Communications Act 2002 (establishing the regulator Ofcom).

Justification for taking the power

337. A power to vary the maximum number of members is needed to ensure that the new governance model works efficiently and effectively. It may be necessary, over time, to make changes to the number of members of the new body so it can adapt to meet its objectives, and ensure that the requisite skills and expertise are at all times represented on the board. It is appropriate that the Secretary of State is able to maintain strategic oversight of the Information Commission as it evolves under its new board structure, as the Secretary of State remains accountable for the costs incurred by the Information Commission, its effectiveness and efficiency, and its strategic direction.

338. Before making regulations under this power the Secretary of State is required to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate (see section 182 DPA 2018).

Justification for the procedure

339. The negative resolution procedure affords an adequate level of parliamentary scrutiny in the case of this Henry VIII power: it gives a narrow power to enable the Secretary of State to alter the maximum number of board members. It is necessary to include such a power in order to ensure that the newly constituted body can perform effectively under its new governance model and, in particular, that the Secretary of State can ensure a diversity of candidates and perspectives are represented on the board while retaining some control over the overall costs incurred by the Information Commission in relation to the remuneration of the membersSection 1(7) and (8) of the Office of Communications Act 2002 sets a precedent for a power of this sort to be subject to the negative resolution procedure.

Schedule 13, paragraph 3(6) of the new Schedule 12A to the DPA 2018: Power to set a maximum and minimum number of executive members by direction

Power conferred on: Secretary of State

Power exercised by: Directions

Parliamentary Procedure: None

Context and Purpose

340. This provision states that the Secretary of State may set a direction as to the maximum and minimum number of executive members.

Justification for taking the power

341. This provision should be read together with paragraph 2 of Schedule 12A, which sets a maximum and minimum number of members of the Commission and enables the Secretary of State to make regulations in order to vary the overall maximum number of members of the board. Within the parameters set by paragraph 2(2) and any regulations under paragraph 2(3), it seems appropriate to give the power to the Secretary of State, if necessary, to determine by a simple direction the maximum and minimum number of executive members, assisting her to fulfil her strategic and financial responsibilities in relation to the Information Commission. The Secretary of State in exercising the power to set a direction must comply with her statutory obligation to secure, so far as practicable, that the number of non-executive members is, at all times, greater than the number of executive members.

Justification for the procedure

342. To ensure the agility and efficiency of the Information Commission, and to ensure a range of skills are represented on the board, it is important that the Secretary of State should have the power to set a simple direction to vary the maximum and minimum number of executive members. There is a precedent for this approach at section 1(6)(a) of the Office of Communications Act 2002.

Department for Science, Innovation and Technology
8 March 2023