HOUSE OF LORDS

Delegated Powers and Regulatory Reform Committee

6th Report of Session 2017–19

Data Protection Bill [HL]

Ordered to be printed 18 October 2017 and published 24 October 2017

Published by the Authority of the House of Lords

HL Paper 29

The Delegated Powers and Regulatory Reform Committee

The Committee is appointed by the House of Lords each session and has the following terms of reference:

(i) To report whether the provisions of any bill inappropriately delegate legislative power, or whether they subject the exercise of legislative power to an inappropriate degree of parliamentary scrutiny;

(ii) To report on documents and draft orders laid before Parliament under or by virtue of:

(a) sections 14 and 18 of the Legislative and Regulatory Reform Act 2006,

(b) section 7(2) or section 19 of the Localism Act 2011, or

(c) section 5E(2) of the Fire and Rescue Services Act 2004;

and to perform, in respect of such draft orders, and in respect of subordinate provisions orders made or proposed to be made under the Regulatory Reform Act 2001, the functions performed in respect of other instruments and draft instruments by the Joint Committee on Statutory Instruments; and

(iii) To report on documents and draft orders laid before Parliament under or by virtue of:

(a) section 85 of the Northern Ireland Act 1998,

(b) section 17 of the Local Government Act 1999,

(c) section 9 of the Local Government Act 2000,

(d) section 98 of the Local Government Act 2003, or

(e) section 102 of the Local Transport Act 2008.

Membership

The members of the Delegated Powers and Regulatory Reform Committee are:

Lord Blencathra (Chairman)
Baroness Dean of Thornton-le-Fylde
Lord Flight
Lord Jones
Lord Lisvane
Lord Moynihan
Lord Rowlands
Lord Thomas of Gresford
Lord Thurlow
Lord Tyler

Registered Interests

Committee Members' registered interests may be examined in the online Register of Lords' Interests at www.publications.parliament.uk/pa/ld/ldreg.htm. The Register may also be inspected in the Parliamentary Archives.

Publications

The Committee's reports are published by Order of the House in hard copy and on the internet at www.parliament.uk/hldprrcpublications.

General Information

General information about the House of Lords and its Committees, including guidance to witnesses, details of current inquiries and forthcoming meetings is on the internet at http://www.parliament.uk/business/lords/.

Contacts for the Delegated Powers and Regulatory Reform Committee

Any query about the Committee or its work should be directed to the Clerk of Delegated Legislation, Legislation Office, House of Lords, London, SW1A 0PW. The telephone number is 020 7219 3103 and the fax number is 020 7219 2571. The Committee's email address is hldelegatedpowers@parliament.uk.

Historical Note

In February 1992, the Select Committee on the Committee work of the House, under the chairmanship of Earl Jellicoe, noted that "in recent years there has been considerable disquiet over the problem of wide and sometimes ill-defined order-making powers which give Ministers unlimited discretion" (Session 1991–92, HL Paper 35-I, paragraph 133). The Committee recommended the establishment of a delegated powers scrutiny committee which would, it suggested, "be well suited to the revising function of the House". As a result, the Select Committee on the Scrutiny of Delegated Powers was appointed experimentally in the following session. It was established as a sessional committee from the beginning of Session 1994–95. The Committee also has responsibility for scrutinising legislative reform orders under the Legislative and Regulatory Reform Act 2006 and certain instruments made under other Acts specified in the Committee's terms of reference.

CONTENTS

Sixth Report

DATA PROTECTION BILL [HL]

Introduction

1. The Data Protection Bill had its second reading on 10 October. It makes new provision to regulate the processing of personal data in the UK in place of the Data Protection Act 1998 (the 1998 Act) which is repealed.[1]

2. **Part 2** of the Bill supplements the so-called "General Data Protection Regulation" (GDPR)[2] on the protection of natural persons with regard to the processing of data and on the free movement of data. The GDPR will apply as from 25 May 2018. It is directly applicable in UK law, and so confers rights which can be enforced by individuals in domestic courts without implementing legislation. It regulates all processing of personal data within the scope of the EU law, other than processing for law enforcement purposes.

3. The GDPR sets out new principles (in Article 5) about the processing of personal data which must be observed by data controllers and processors. For example, the data must be processed "lawfully, fairly and in a transparent manner in relation to the data subject". It also gives data subjects a number of specific legal rights. In particular:

    - Articles 13 and 14 confer a right of access to personal data held by a controller;
    - Article 16 confers a right to rectification of inaccurate data;
    - Article 17 contains a right to erasure of data on certain grounds–for example, where it is no longer necessary for the controller to retain the data.

4. The GDPR allows Member States to pass legislation providing for exemptions from some of those principles and rights. Schedules 2 to 4 of the Bill lists the exemptions that will apply in the UK.

5. The GDPR also forbids the processing of particularly sensitive types of personal data or the transfer of any type of personal data to countries outside the EU unless (in each case) certain strict conditions and safeguards apply. These provisions are supplemented by Schedule 1 to the Bill (sensitive personal data) and regulations to be made under clause 17 (transfer of data to third countries etc.) respectively.

6. Chapter 3 of Part 2 of the Bill regulates law enforcement data processing in areas outside the scope of EU law[3] by applying the GDPR.

7. **Part 3** of the Bill concerns the so-called "Law Enforcement Directive" (LED)[4] on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention,

1 The Data Protection Act 1998 implemented Directive 95/46/EC which is repealed by the GDPR.
2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
3 Except for data processing by the intelligence services, which is dealt with by Part 4 of the Bill.
4 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.

investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. The LED is not directly applicable: Member States have to transpose it into domestic law by 6 May 2018.[5] This is achieved by Part 3 of the Bill.

8. **Part 4** of the Bill regulates data processing by the UK intelligence services. This is outside the scope of EU law, but it does fall within the scope of Council of Europe Convention 108 ("Convention 108") for the protection of individuals with regard to automatic processing of personal data. Negotiations on a revised Convention 108 are currently underway, although a final text is yet to be agreed. Part 4 of the Bill seeks to implement the proposed new Convention in relation to data processing by the intelligence services.[6]

9. The data protection regimes provided for in the GDPR and Parts 2 to 4 of the Bill place wide-ranging obligations on "controllers" in relation to the "processing" of "personal data". These terms are defined very widely in the GDPR:

- "controllers" means "the natural or legal person, public authority, agency or other body which alone or jointly with others, determines the purposes or means of the processing of personal data";
- "processing" means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction";
- "personal data" means any information relating to an identified or identifiable natural person (who is referred to as the "data subject").

The legislation will thus apply to every business or public or private sector organisation in the country, regardless of size, which collects or holds data about identifiable individuals.[7]

10. **Parts 5 and 6** of the Bill are about the Information Commissioner. He or she is given extensive enforcement powers to investigate suspected breaches of the legislation, and to serve enforcement and assessment notices. The Commissioner may also impose very substantial penalties: up to the higher of €10 million or 2% of an undertaking's turnover or, in relation to certain types of failures, €20 million or 4% of turnover.[8]

11. The Department for Digital, Culture, Media and Sport has provided a lengthy memorandum about the delegated powers in the Bill,[9] which include several widely-drafted and highly significant Henry VIII provisions.

---

5 Under the European Union (Withdrawal) Bill, both the GDPR and LED become "retained EU law" and would therefore continue to have effect in the UK after exit day unless and until repealed or amended by further domestic legislation.

6 The requirements of the Convention 108 concerning the processing of personal data by other data controllers are implemented in the UK by the GDPR and Parts 2 and 3 of the Bill.

7 The legislation does not, however, apply to the processing of personal data by an individual in the course of a purely personal or household activity.

8 See Article 83 of the GDPR and clause 150 of the Bill.

9 Department for Digital, Culture, Media and Sport and the Home Office, *Data Protection Bill [HL]: Delegated Powers Memorandum*: https://publications.parliament.uk/pa/bills/lbill/2017–2019/0066/18066-DPM.pdf

The memorandum justifies many of the powers simply on the basis that "flexibility" is needed to deal with future changes of circumstances. **We are troubled that the Government should think it appropriate, on the basis of such a thin justification, to seek to take wide-ranging powers allowing current or future Ministers to implement important policy changes without the need for further primary legislation.**

12. In this report, we draw the following provisions to the attention of the House:

- Clause 9(6)
- Clauses 11 and 51
- Clauses 15 and 111
- Clause 17
- Clause 21
- Clauses 33(6) and 84(3)
- Clause 132(1) and (6)
- Clauses 142(8) and 148(5)
- Clause 151(1)
- Clause 153(1)
- Clause 170(1)

Clause 9(6)—Power to add, vary or omit conditions or safeguards applying to the processing of sensitive personal data

13. Article 9 of the GDPR contains strict rules about the processing of personal data which "reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership" and the processing of "genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

14. The processing of sensitive personal data is prohibited except in the circumstances set out in Article 9 itself, or in legislation passed by Member States which must (a) be "necessary for reasons of substantial public interest", and (b) include "suitable and specific measures to safeguard the fundamental rights and the interests of the data subjects".

15. Schedule 1 to the Bill provides for 28 distinct cases in which processing of this type of sensitive data will be permitted in the UK, including processing that is necessary "for health or social care purposes" or "for reasons of substantial public interest in the exercise of a function of either House of Parliament", or "for the purposes of prevention or detection of an unlawful act".[10] These cases apply only if specified conditions are met and safeguards observed: for example, processing of personal data revealing someone's racial origin or sexual orientation for the purpose of identifying absence of equality of treatment is not lawful if it would cause an individual substantial

10 See Sch 1, paras 2, 6 and 8.

damage or distress.[11] In all the cases, the data controller must have in place the safeguards referred to in Part 4 of Schedule 1, in particular controllers must produce a document explaining their policies for securing compliance with the data protection principles laid down in the GDPR.

16. However, clause 9(6) contains a Henry VIII power to allow the Secretary of State, by affirmative procedure regulations, to amend Schedule 1 by "adding, varying or omitting conditions or safeguards" and to make consequential amendments to clause 9 itself.

17. The memorandum[12] asserts that the power is based on existing provisions in Schedule 3 to the 1998 Act under which Ministers may by affirmative procedure order:

- allow sensitive personal data to be processed in circumstances other than those set out in that Schedule;
- modify certain existing conditions in that Schedule which allow for sensitive data to be processed in three specified categories of cases (those relating to employment, administration of justice and monitoring of equal opportunities).

18. The memorandum continues:

> "The power to amend or remove conditions is based on those powers, though it is drawn slightly wider. It is necessary to enable safeguards for data subjects to be added to or adapted, where it becomes apparent that the conditions and safeguards provided in Schedule 1 do not provide sufficient protection for data subjects, or where the conditions and safeguards need updating to deal with changing circumstances. Exercise of the power would be subject to the [conditions in Articles 9 and 10 of the GDPR] which require, for example, that the safeguards provided are appropriate."

19. We do not agree that the power conferred by clause 9(6) is only "slightly" wider than the existing ones in Schedule 3 to the 1998 Act. The new power would allow the Government by regulations completely to rewrite all the conditions and safeguards about the processing of special categories of data in Schedule 1 to the Bill. In contrast, the 1998 Act only permits new conditions to be added or three existing ones to be modified.

20. In any event, **we take the view that the memorandum does not adequately justify the breadth of the power in clause 9(6) of the Bill, and that it is inappropriate for Ministers to be given carte blanche to rewrite any or all of the conditions and safeguards in Schedule 1 by regulations in order "to deal with changing circumstances" instead of bringing forward a Bill.** While the affirmative procedure would apply to the regulations, this would allow no opportunity for either House to amend what might well be highly controversial provisions—allowing for the most sensitive types of personal data to be processed in entirely new circumstances.

21. **We consider that clause 9(6) is inappropriately wide and recommend its removal from the Bill.**

---

11 See Sch 1, para 7(4).
12 Paras 23 to 26.

22. **It may be appropriate, however, for Ministers to have a more focused power enabling them to update specific paragraphs in Schedule 1 as result of changes to other legislation (for example, the references to criminal justice laws in paragraph 27). The Government may wish therefore to consider which particular provisions in that Schedule might need to be changed if this approach were to be adopted.**

Clauses 11 and 51—Power to specify maximum fees

23. Article 12(5) of the GDPR allows controllers to charge "reasonable fees" for dealing with "manifestly unfounded or excessive" requests from data subjects for access to personal data "taking into account the administrative costs of providing the information or communication or taking the action requested". Article 15(3) allows controllers to charge "a reasonable fee based on administrative costs" for providing more than one copy of personal data undergoing processing.

24. However clause 11(1) in Part 2 of the Bill allows the Secretary of State to make negative procedure regulations specifying a cap on fees that may be charged by controllers for those purposes.

25. Similarly clause 51(4) in Part 3 of the Bill, which is intended to implement Article 12 of the LED, allows the Secretary of State to impose a cap on fees charged by law enforcement data controllers for dealing with manifestly unfounded or excessive requests for access to personal data.

26. The GDPR and LED each confer a right on controllers to charge reasonable fees for dealing with excessive requests, taking into account their administrative costs. Yet clauses 11 and 51 would allow for those rights to be modified, so that controllers may not be able to recover their reasonable costs in full.

27. **We draw these provisions to the attention of the House, which may wish to ask the Minister to explain why he or she considers that a cap on fees charged by controllers would be authorised by the GDPR and the LED.**

Clauses 15 and 111—Power to make further exemptions in relation to the rules about the processing on personal data

28. The GDPR[13] allows Member States to pass legislation providing for exemptions from, and restrictions and adaptations to, specified data protection principles and data subject rights. For the most part, these have to be (a) for purposes of general public interest, and (b) subject to appropriate safeguards.

29. Schedules 2 to 4 to the Bill set out the exemptions that will apply in the UK. For example, certain data protection principles and provisions such as individuals' right of access of personal data held about them by a controller will not apply if there would be prejudice to:

- an investigation into whether the data subject had committed a criminal offence;[14] or
- the maintenance of effect immigration control.[15]

13 See Articles 6(3), 23(1), 85(2) and 89(2) and (3) of the GDPR.
14 Para 2 of Sch 2.
15 Para 4 of Sch 2.

30. Clause 15(2) in Part 2 of the Bill confers a power on the Secretary of State, by affirmative procedure regulations, to provide for further exemptions from the obligations and rights set out in the GDPR. This is a Henry VIII power because the regulations may amend or repeal any provision in clause 14 of and Schedules 2 to 4 to the Bill.

31. Part 4 of the Bill regulates the intelligence services. They will be required to process data consistently with six principles laid in down in clauses 84 to 89. Clauses 90 to 98 confer various rights on data subjects, for example a right to seek information from the data controller. Clause 108 set out exemptions for the purpose of safeguarding national security. Schedule 11 sets out further exemptions, for example in relation to processing carried out for the purposes of the detection and prevention of crime.

32. Clause 111 confers a power analogous to that in clause 15(2). It enables the Secretary of State, by affirmative procedure regulations, to provide for further exemptions from any provisions of Part 4. This is also a Henry VIII power, because clause 111(2) allows the regulations to amend or repeal any provision of Schedule 11. According to the memorandum, the power would be used "if the Secretary of State considers that the exemption is necessary for safeguarding the interests of data subjects or the rights and freedoms of others";[16] but clause 111 itself contains no such limitation on the circumstances in which the power could be used.

33. The memorandum gives the following justification for these powers:

> "The Bill exercises these derogations to reflect current public policy, but this is subject to change over time. Flexibility is required, including after the UK leaves the EU when the regulation-making power in section 2(2) of the European Communities Act 1972 will no longer available, to enable the UK to make full use of the permissible derogations[17], including by adapting (and, if necessary, amending existing provision in clause 14 and Schedules 2 to 4) or extending these derogations in the light of changing public policy requirements."[18]

34. **We regard this is an insufficient and unconvincing explanation for such an important power. As we have observed in several reports, it is not good enough for Government to say that they need "flexibility" to pass laws by secondary instead of primary legislation without explaining in detail why this is necessary—particularly in the case of widely-drawn Henry VIII powers.**[19] **While we recognise that the affirmative procedure would apply to regulations under clauses 15 and 111, this is not an adequate substitute for a Bill allowing Parliament fully to scrutinise proposed new exemptions to data obligations and rights**.

35. **We consider that the delegations of power in clauses 15 and 111 are inappropriately wide, and recommend their removal from the Bill.**

---

16 Para 45.

17 Section 2(2) of the European Communities Act 1972 would allow Ministers to make regulations providing for further derogations from the GDPR; but that power will disappear as from exit day: see section 1 of the EU (Withdrawal) Bill.

18 Para 46.

19 See in particular Delegated Powers and Regulatory Reform Committee, *Special Report: Quality of Delegated Powers Memoranda* (7th Report, Session 2014–15, HL Paper 39), Appendix 4, paras 29 and 35.

36. **However, as with clause 9, it may be appropriate for Ministers to have a more focused power enabling them to update specific paragraphs in Schedules 2, 3, 4 and 11 as result of changes to other legislation (for example, the reference to the NHS Redress Act 2006 in paragraph 8 of Schedule 2). Again, the Government may wish to consider which particular provisions in these four Schedules might need to be changed if this approach were to be adopted**.

Clause 17—Power to make provision in respect of transfers of personal data to third countries and international organisations

37. Chapter 5 of the GDPR places strict restrictions on the transfer of personal data to a third country (that is, a non-EU Member State) or an international organisation. Generally such transfers require the EU Commission to have decided that the third country or international organisation ensures an adequate level of data protection. However Article 49(1) provides for other limited grounds for transferring personal data to third countries or international organisations, one of which being that the transfer is necessary for important reasons of public interest specified in legislation passed by Member States.

38. The Bill itself does not itself set out any such public interest reasons. Instead clause 17(1) confers a power on the Secretary of State by negative procedure regulations to specify:

- circumstances in which a transfer of personal data to a third country or international organisation *is* to be taken as necessary for an important reason of public interest; and
- circumstances in which such a transfer *is not* to be taken as necessary for an important reason of public interest.

39. Article 49(5) of the GDPR applies where the EU Commission has not made a decision that a particular third country or international organisation has an adequate level of data protection safeguards in place. Member States are allowed by legislation to set limits on the transfer of specific categories of personal data to that third country or international organisation where it is necessary for important reasons of public interest to impose this restriction. Clause 17(2) of the Bill would enable restrictions in the UK to be imposed by the Secretary of State by negative procedure regulations.

40. These two sets of significant powers are justified in the memorandum on the basis that it is not possible for the Government to identify and set out all current and future matters of public interest in the Bill.[20] While this is not a persuasive explanation, we accept that these are matters that are appropriately dealt with in secondary legislation.

41. The negative procedure is justified on the basis that "the framework for the transfer of personal data to third countries is provided for in the GDPR and that any regulations would serve to amplify the application of the public interest test provided for in Article 49".[21]

20 Para 51.
21 Para 53.

42. **In our view, however, the negative procedure is not the appropriate procedure for regulations specifying that the transfer of data to third countries or international organisations is to be regarded as necessary in the public interest. We anticipate that the House would wish to debate as a matter of course provisions of this type, for example regulations which declared that, for example, it is to be treated as necessary in the public interest to transfer bulk personal data held by a UK Government department to the agencies of a foreign power.**

43. **We therefore recommend that the affirmative procedure should apply to regulations made under clause 17(1)(a).**

Clause 21—Power to make provision in consequence of regulations related to the GDPR

44. Chapter 3 of Part 2 of the Bill applies the GDPR to all areas of data processing in the UK which are outside the scope of EU law, apart from data processing regulated by Part 4 (UK intelligence services). The areas covered by this so-called "applied GDPR" include, according to the memorandum, national security, foreign policy, defence and some immigration activities.[22]

45. The derogations and exemptions set out in Chapter 2 of Part 2 of the Bill will extend to "the applied GDPR" (with certain modifications set out in Schedule 6) as will all the regulation-making powers in Chapter 2.

46. Clause 21(1) confers a power on the Secretary of State, by affirmative procedure regulations, to make provisions for "the applied GDPR" equivalent to those made by regulations under section 2(2) of the European Communities Act 1972 ("the 1972 Act") in respect of the GDPR itself. This is a Henry VIII power because the regulations may amend or repeal any provision of "the applied GDPR", or of Chapter 3 of Part 2 of the Bill, or of Parts 5 to 7, in so far as they relate to the applied GDPR.[23]

47. The memorandum explains:

> "Although it is not currently anticipated that regulations will need to be made under the 1972 Act [in respect of the GDPR], the purpose of the power [in clause 21(1)] is to ensure that, should any regulations be made under the 1972 Act, it will be possible to make regulations for the applied GDPR as well. This helps to ensure consistency between the regimes."[24]

48. We are nonetheless puzzled by the inclusion of clause 21. Chapter 2 of Part 2 confers a suite of delegated powers on Ministers to provide by regulations for various exemptions and derogations from the obligations and rights contained in the GDPR which, as noted above, may also be exercised in respect of "the applied GDPR". The memorandum fails to explain why those powers are considered inadequate, or why the Government might need to have recourse to the distinct powers in section 2(2) of the 1972 Act—which allows Ministers to make regulations:

> "for the purpose of implementing any EU obligation of the United Kingdom, or enabling any such obligation to be implemented, or of

22 Para 8.
23 See clause 21(4).
24 Para 54.

enabling any rights enjoyed or to be enjoyed by the United Kingdom under or by virtue of the [EU] Treaties to be exercised".

49. Clause 1 of the European Union (Withdrawal) Bill provides for the repeal of the 1972 Act as from exit day which, it is anticipated, will be on 29 March 2019.

50. Clause 21(1) therefore appears to have been included just in case the Government decide that, between the date of Royal Assent for this Bill and 29 March 2019, they do need after all to make regulations under section 2(2) of the 1972 Act instead of under the powers in Chapter 2 of Part 2 of the Bill.

51. **We consider it unsatisfactory that the Government should seek to take this widely drafted power without explaining properly what it might be used for; and we therefore recommend the removal of clause 21 from the Bill unless the Government can provide, to the satisfaction of the House, a full and convincing justification as to why is both necessary and appropriate.**

Clauses 33(6) and 84(3)—Power to amend Schedules 8 and 10 by adding, varying or omitting conditions for sensitive processing

52. Clause 33, in Part 3 of the Bill, sets out the first data protection principle governing the processing of personal data for law enforcement purposes, namely that the processing must be lawful and fair. In determining the lawfulness of processing, additional safeguards apply where the personal data is particularly sensitive, for example, data revealing a person's racial or ethnic origin. "Sensitive processing" is only permissible if it is strictly necessary, and it meets one of the conditions in Schedule 8.

53. Paragraphs 2 and 3 of Schedule 8 transpose two conditions expressly provided for in Article 10 of the LED, namely to protect the data subject's vital interests or where the personal data is already in the public domain. Article 10 also allows further conditions to be specified in legislation passed by the Member States. Paragraphs 1 and 4 to 6 of Schedule 8 to the Bill therefore specifies a number of further conditions (which replicate conditions in Article 9(2) of the GDPR).

54. Clause 33(6) confers a Henry VIII power to allow the Secretary of State, by affirmative procedure regulations, to amend Schedule 8 by adding, varying or omitting conditions.

55. Schedule 10 makes equivalent provision in respect of the conditions applicable to sensitive processing under Part 4 of the Bill which applies to the intelligence services. Clause 84(3) contains a Henry VIII power analogous to that in clause 33(6) to allow the Secretary of State to add, vary or omit conditions in Schedule 10.

56. **The memorandum gives a weak justification for clauses 33(6) and 84(3). This is that (a) "the regulation-making powers afford the flexibility to specify additional conditions in the light of changing circumstances", and (b) they mirror the power at paragraph 10 of Schedule 3 to the 1998 Act.**[25]

25 Para 68.

57. **For essentially the same reasons that we give above in relation to clause 9(6), we consider it inappropriate for the Bill to confer such widely drawn and far-reaching powers; and we therefore recommend the removal of clauses 33(6) and 84(3).**

58. **It may be again appropriate, however, for the Government to have narrower power to allow for the up-dating of specific provisions in Schedules 8 and 10 without the need for primary legislation.**

Clause 132(1) and (6)—Power to require controllers to pay specified charges and to provide information to the Commissioner

59. Clause 132(1) to (3) confers a power on the Secretary of State, by regulations, to require data controllers to pay charges to the Information Commissioner of an amount specified in regulations. The affirmative procedure will apply, unless the regulations merely increase charges specified in previous regulations to reflect inflation.

60. Clause 132(6) enables regulations to be made, also under the affirmative procedure, requiring data controllers to provide information to the Commissioner so that he or she can determine whether a charge is payable and, if so, how much.

61. Clauses 132 and 133 replicate and replace sections 108 to 110 of the Digital Economy Act 2017 ("the 2017 Act")[26] with a view to ensuring that all provisions relating to the Commissioner's data protection functions are in the same piece of primary legislation.[27] However, an important difference in the new provisions is that a failure by a data controller to pay the charges or to provide information required by the regulations could result in enforcement action by the Commissioner, including the imposition of a substantial penalty: see below.

62. As we noted in our report on the Digital Economy Bill, these are highly significant powers:[28] almost every organisation is likely to be a data controller, including all commercial businesses (large or small), charities, voluntary groups, Government departments, local authorities, hospitals—and each House of Parliament, and individual members of those Houses. Regulations under clause 132 of the Bill could require every data controller in the UK to pay charges and provide information to the Commissioner.

63. The charges will be free-standing, in that they need not relate to any service provided by the Commissioner to data controllers; and the regulations may make provision about the times or periods within which a charge must be paid, and for different charges to be payable in different cases.

64. The background to the introduction of the new charging system was explained in the delegated powers memorandum on the provisions which became section 108 to 110 of the 2017 Act. In summary:

- Part 3 of the 1998 Act requires data controllers (subject to certain exceptions) to provide a notification to the Commissioner and

26 Added by Government amendments at Lords Report stage of the Bill for the Digital Economy Act 2017. No regulations have been made so far under sections 108 to 110 of that Act.

27 See the delegated powers memorandum, para 109.

28 Delegated Powers and Regulatory Reform Committee (21st Report, Session 2016–17, HL paper 139), paras 26 to 39.

be included on a register. They must also apply annually to the Commissioner to remain on the register.

- Notification applications to the Commissioner must be accompanied by the fee prescribed by regulations made under Part 3. Those fees fund the expenses incurred by the Commissioner in carrying out his functions under the 1998 Act.

- However Part 3 of the 1998 Act is to be repealed with effect from 25 May 2018 when the GDPR comes into force. The GDPR (unlike the existing Data Protection Directive which the 1998 Act implements) does not contain a requirement for national data protection authorities to maintain a register of data controllers.

- The new clauses therefore confer a free-standing power on the Secretary of State to make regulations to provide funds for the Information Commissioner.

65. Our report on the Bill for the 2017 Act contained a number of recommendations about the new regulation-making powers, for example as regards consultation and Parliamentary procedure. With one important exception, these recommendations were accepted by the Government and have been carried forward into clauses 132 and 133 of this Bill.

66. However the Government did not accept one key recommendation. This was that, in determining the amount of changes to be specified in regulations, the Secretary of State should ensure that the income from them does not exceed the reasonably anticipated costs of discharging the data protection functions of the Commissioner and the Secretary of State.

67. This was our rationale for that recommendation:

> "In making the regulations, the Secretary of State must "have regard to the desirability of securing that the charges payable are sufficient to offset expenses incurred by [the Information Commissioner and Secretary of State in discharging certain functions under the 1998 Act, the General Data Protection Regulation and in doing other specified things]". But there is nothing expressly to prevent the Secretary of State from specifying charges intended to recover a surplus over the costs incurred in discharging the functions specified. We are concerned that current or future Ministers might wish to use the power to levy charges to fund a wider range of functions—as has happened with broadly similar legislation enabling the Government to prescribe enhanced court fees, which they are relying on to introduce large increases in probate fees."[29]

68. In their response, the Government said:

> "We have considered carefully the Committee's recommendation to make it a requirement for the Secretary of State in determining the amount of charges, to ensure that the income from them does not exceed the reasonably anticipated costs of discharging the specified functions of the Information Commissioner and Secretary of State related to data protection. It is the Government's view that the limited flexibility given in the Government's amendments is necessary given rapid developments

29 Delegated Powers and Regulatory Reform Committee (21st Report, Session 2016–17, HL Paper 139), para 34.

> in the digital economy and to manage the inevitable period of transition as the [Information Commissioner] takes on additional responsibilities under the forthcoming General Data Protection Regulation. The language used in the Government's amendment mirrors that in the existing Data Protection Act. Parliament has not expressed any concerns about how the existing powers have been exercised and we believe that by subjecting each exercise of the power to the affirmative procedure we are putting in place sufficient Parliamentary safeguards to ensure the powers will be exercised in a rational and responsible way in the future. We therefore do not intend on tabling an amendment to address this recommendation."[30]

69. It seems implicit from this that the Government want to retain the flexibility to impose charges on data controllers that would generate funds in excess of the amount needed to fund the functions of the Commissioner and Secretary of State in relation to data protection—perhaps in order to cross-subsidise the cost of other activities, for example the Commisioner's functions under the Freedom of Information Act 2000.

70. **We remain firmly of the view that it is unacceptable for the Government to have power to impose tax-like charges by secondary legislation. We therefore recommend the amendment of clause 132(4)[31] so as to prohibit regulations that set charges designed to generate excess funds.**

Clauses 142(8) and 148(5)—Power to confer power on the Commissioner to give an enforcement notice or a penalty notice in respect of other failures

71. Under clause 142(1), the Information Commissioner may serve an enforcement notice where he or she is satisfied that a person has failed to comply with a provision of the GDPR or the Bill listed in subsections (2) to (5), for example where a controller had not taken sufficient measures to prevent the accidental loss of personal data.[32] A failure to comply with an enforcement notice can result in the imposition of a penalty under clause 148.

72. Clause 142(8) enables the Secretary of State, by affirmative procedure regulations, to add to the types of failures which may trigger the issue of an enforcement notice. It is a Henry VIII power because the regulations may amend clause 142 itself and clauses 143 to 146[33]. These need not necessarily be failures to comply with a provision of the GDPR or of the Bill.

73. Under clause 148(1), the Commissioner may give a penalty notice to a person:

- in the same circumstances in which an enforcement notice may be issued;

30 Delegated Powers and Regulatory Reform Committee (24th Report, Session 2016–17, HL Paper 149), Appendix 1.

31 Clause 132(4) is materially identical to the corresponding provision in the Digital Economy Act 2017, namely section 109(2).

32 This would be a failure to comply with the principle in Article 5(1)(f) of the GDPR.

33 Clauses 143 to 146 make supplementary provision about enforcement notices, the rectification and erasure of personal data, restrictions on the giving of enforcement notices and the cancellation and variation of such notices

- where there has been non-compliance with an assessment notice;[34] or
- where there has been non-compliance with an enforcement notice.

74. Clause 148(5) allows the Secretary of State to make affirmative procedure regulations conferring power on the Commissioner to issue a penalty notice in respect of failures other than those listed in subsection (1)—which again need not necessarily be a failure to comply with a provision of the GDPR or the Bill—and to make provision about the amount of penalty that may be imposed. This is also a Henry VIII power because the regulations may amend clause 148 itself and clauses 149 to 151.[35]

75. The following justification is given in the memorandum:

> "The Bill provides for a wide range of circumstances where the Commissioner may issue an enforcement notice (and, if appropriate, a penalty notice), including in respect of a failure to adhere to the principal obligations placed on data controllers and processors. Nonetheless, the Bill imposes other duties on controllers, processors and others where a failure does not attract the power to issue an enforcement notice or a penalty notice. It may be that in the light of operational experience with the new data protection regulatory framework the Secretary of State (following consultation with the Commissioner), considers that other failures warrant the issue of an enforcement notice. These regulation-making powers provide the flexibility needed to extend the power to issue enforcement notices and penalty notices where necessary and enables this to happen relatively speedily should any gap in the enforcement framework be identified."[36]

76. **In our view, this is an inadequate justification for these important provisions. We regard it as inappropriate for the Secretary of State to have an unlimited power to determine:**

- **which types of additional failure should attract the Commissioner's wide enforcement powers; and**
- **the amount of the penalties the Commissioner may impose without any maximum limit.**

77. **We therefore recommend that clauses 142(8) and 148(5) are amended so that:**

- **the Secretary of State may extend the Commissioner's enforcement notice and penalty notice powers only in respect of additional categories of "failure" described, at least in general terms, on the face of the Bill; and**
- **the maximum penalty for the further types of failure is also specified in the Bill.**

---

34 Under clause 140, the Commissioner may serve an assessment notice on a controller or processor so as to allow the Commissioner to assess whether there has been compliance with data protection legislation.

35 Clauses 149 to 151 are concerned with restrictions on the giving of penalty notices, the maximum amount of a penalty, and penalties for non-compliance with charges regulations made under clause 132.

36 Para 125.

78. The affirmative procedure should still apply to the power as so narrowed.

Clause 151(1)—Duty to publish document specifying the amount of the penalty for a failure to comply with charging regulations

79. As noted earlier in this report, clause 132 allows the Secretary of State to make regulations requiring data controllers to pay charges and provide information to the Information Commissioner. A controller who fails to comply with a requirement may be served with an enforcement notice under clause 142 or a penalty notice under clause 148.

80. Clause 151 requires the Commissioner to publish a document setting out the penalty that may be imposed for failure to comply with regulations under clause 132.[37] The document may also specify different penalties that will apply in different cases. It has to be published and laid before Parliament, but it is not subject to any Parliamentary procedure.

81. This is the justification given in the memorandum:

> "The Government considers it appropriate to set the maximum amount of the penalty (through a combination of the formula in clause 151(3) and regulations made under clause 132) but otherwise to leave it to the Commissioner to determine the charge, to allow flexibility to set different charges in different cases and if necessary to adjust the penalty if it is not proving a sufficient deterrent (subject always to the maximum).
>
> The document must be laid before Parliament but it is not otherwise subject to any parliamentary process. This approach is considered appropriate given that the maximum amount of the penalty is provided for through a combination of provisions on the face of the Bill and regulations made under clause 132 which are subject to parliamentary scrutiny."[38]

82. **We regard it as unacceptable for the Commissioner to have the power to determine the amount of penalties that apply where data controllers fail to pay charges or provide information to him or her under clause 132. We recommend that the scale of penalties should be out set in the regulations themselves made under that clause, which are subject to the affirmative procedure, rather than being left to the discretion of the Commissioner with no Parliamentary scrutiny.**

Clause 153(1)—Guidance about regulatory action

83. Clause 153(1) places a duty on the Information Commissioner to prepare and publish guidance about the exercise of his or her functions in connection with assessment notices, enforcement notices and penalty notices. The document has to include guidance:

- about the circumstances in which the Commissioner would consider it appropriate to issue a penalty notice;
- explaining how the Commissioner will determine the amount of penalties (see subsection (5)).

37 This may not, however, exceed 150% of the highest charge payable by a controller in respect of a financial year provided for in the regulations, disregarding any discount available (see subsection (3)).

38 Paragraphs 128 and 129.

84. The guidance must be laid before Parliament, but it is not subject to any Parliamentary procedure. The justification given in the memorandum is that:

> "The Commissioner's enforcement powers are set out on the face of the GDPR and the Bill. The guidance issued under clause 153 cannot add to or otherwise amend those powers, it will simply inform data controllers and others of the Commissioner's approach to the exercise of the powers. In these circumstances, it is not considered necessary to subject the guidance to formal parliamentary scrutiny".[39]

85. Clause 153 appears to be based on section 55C of the 1998 Act. That section requires the Commissioner to prepare and issue guidance about the exercise of the monetary penalty functions conferred on the Commissioner by section 55A—which allows penalties not exceeding £500,000 to be imposed on controllers who breach specified requirements of the 1998 Act. Guidance under section 55C has to be laid before Parliament, but neither the affirmative nor the negative procedure applies.

86. We are nonetheless concerned that Parliament is given no opportunity to scrutinise this highly significant guidance under clause 153. The Commissioner is to have extensive new enforcement powers under the GDPR and the Bill. His or her powers to impose financial penalties is increased from only £500,000 to the higher of €10 million or 2% of an undertaking's turnover or, in some cases, €20 million or 4% of turnover. The guidance will play a central role in the determination of the level of those penalties, and on any review of those penalties by the First-tier Tribunal if an appeal is brought.

87. **We therefore recommend that the guidance should be subject to some form of Parliamentary procedure. On this occasion, we take the view that the negative procedure would be appropriate. This means that the guidance (and future revisions to the guidance) would have laid to be in draft before Parliament, and could not be promulgated before the end of the 40-day prayer period, during which time either House may resolve that it should not come into force.**

Clause 170(1)—Power to reflect changes to the Data Protection Convention

88. Part 4 of the Bill provides for processing of personal data by the Intelligence Services. It is designed to reflect the requirements of the proposed new Council of Europe Convention 108 on the protection of individuals with regard to automatic processing, which is still being negotiated.[40]

89. Clause 170(1) confers a power on the Secretary of State, by affirmative procedure regulations, to make such provision as he or she considers "necessary or appropriate in connection with an amendment of, or instrument replacing, the [existing Convention 108] which has effect, or is expected to have effect in the United Kingdom".

90. This is a Henry VIII power: subsection (2) allows for the regulations to amend any provision of Bill itself (not just Part 4) for example, by amending the functions of the Information Commissioner in Parts 5 and 6. It would

39 Paragraph 142.
40 This will replace the existing version of the Convention concluded in 1981.

also permit the Government to make free-standing regulations to implement a replacement Convention, or changes to the existing Convention, without amending the Bill itself.

91. The memorandum explains that the power to amend the Bill needs to go beyond the provisions in Part 4 because:

- certain other provisions in the Bill also derive from Convention 108;[41] and
- "following the UK's withdrawal from the EU, the modernised Convention 108 could impact on the GDPR and applied GDPR schemes, necessitating amendments to Part 2 of the Bill".[42]

92. The memorandum goes on to say:

> "The Council of Europe is in the process of revising Convention 108, with negotiations on a replacement Convention being well advanced. However, until the text of the revised Convention has been agreed, relevant provisions of the Bill must necessarily be based on the current draft of the text of the modernised Convention 108. Given that a revised Council of Europe data protection Convention is in prospect, it is necessary to have a power to amend relevant provisions of the Bill to ensure that they fully reflect the terms of the modernised Convention 108 as eventually agreed by the Council of Europe … While it would have been preferable for the modernised Convention 108 to have been agreed before the Bill's introduction, this is not the case and it is therefore considered appropriate that a power should be taken to amend relevant provisions in the Bill should the final text of the revised Convention 108 materially depart from the existing draft text. If the revised Convention 108 is agreed during the passage of the Bill, the Government will consider the continued necessity for this power."[43]

93. We agree that it is appropriate for the Secretary of State to have a power by regulations to amend Part 4 of the Bill, and other provisions relating to Part 4, so as to ensure that the UK's obligations under the final text of Convention 108 can be fully implemented in domestic law without the need for further primary legislation. However, the power conferred by clause 170 goes much wider than this: it allows the Secretary of State to make such provision by regulations as he or she considers necessary or appropriate in connection with an amendment to Convention 108 (that is, to the existing 1981 Convention) or to an instrument replacing the Convention.[44] As the memorandum acknowledges, this would even enable the Government to amend Part 2 of the Bill as a result of EU withdrawal, presumably because the requirements of the Convention might apply in place of EU obligations.

94. The Government could also use the power in the future to amend any provision of the Bill to reflect changes to Convention 108 in the event that, for whatever reason, the existing Convention is not replaced by an entirely new instrument.

---

41 For example, relating the functions of the Commissioner as set out in Sch 13 and Part 2 of Sch 14.
42 Para 144.
43 Para 145.
44 The power could not be used, however, to implement amendments to a replacement Convention.

95. **In our view the power is inappropriately wide. We therefore recommend that clause 170 is amended so that the power:**

- **could be used only to make changes to Part 4, and provisions related to Part 4, that are necessary to reflect the final version of modernised Convention 108; and**
- **is time-limited so that it could not be exercised after the expiry of three years from the date of Royal Assent.**

APPENDIX 1: MEMBERS AND DECLARATIONS OF INTERESTS

Committee Members' registered interests may be examined in the online Register of Lords' Interests at www.publications.parliament.uk/pa/ld/ldreg.htm. The Register may also be inspected in the Parliamentary Archives.

For the business taken at the meeting on 18 October 2017 Members declared no interests.

Attendance

The meeting on the 18 October 2017 was attended by Lord Blencathra, Baroness Dean of Thornton-le-Fylde, Lord Flight, Lord Jones, Lord Moynihan, Lord Rowlands, Lord Thomas of Gresford and Lord Tyler.