EVIDENCE ON THE DATA PROTECTION BILL

For the House of Commons Public Bill Committee by
Open Rights Group and Chris Pounder

March 2018

Open Rights Group is a digital rights campaigning organisation. Campaigning for a world where we each control the data our digital lives create, deciding who can use it and how, and where the public's rights are acknowledged and upheld.

Contacts:

Javier Ruiz
Policy Director
Open Rights Group
02070961079
javier@openrightsgroup.org

Slavka Bielikova
Policy Officer
Open Rights Group
02070961079
slavka@openrightsgroup.org

Contents:

Collective redress - Article 80(2) of the GDPR

1. Open Rights Group campaign for a world where we each control the data our digital lives create, deciding who can use it and how, and where the public's rights are acknowledged and upheld.

2. With these principles in mind, Open Rights Group calls for amendments to Clause 183 to strengthen enforcement of data subjects' rights in the Data Protection Bill.

3. Clause 183 gives effect to Article 80(1) of the GDPR, enabling data subjects to authorise a body, or other organisation which meets the conditions set out in Article 80 of the GDPR, to exercise certain rights on the data subject's behalf.

4. While welcome, this approach would require individuals to be aware that they are a victim of a breach of the law, which often people are not. These proposed amendments would enable organisations such as Open Rights Group to take action 'independently of a data subject's mandate', if it considers that the rights of a data subject have been breached.

Data protection rights should be as enforceable as consumer rights

5. In consumer law there is a power for private enforcers to take civil actions in courts to protect the collective consumer rights via enforcement orders. Which? are the only designated private enforcer.

6. In the financial sector, there is a power for Which?, Citizens Advice, the Federation of Small Businesses and the Consumer Council for Northern Ireland to present "super-complaints" to the Financial Conduct Authority.

7. Following the passage of the Bill in the House of Lords, the Government responded to calls to include Article 80(2) of the EU General Data Protection Regulation on providing collective representation of data subjects with an amendment that would only allow its implementation after a review of a different article (Article 80(1)).

8. In our opinion, this review is unnecessary and may not provide relevant information to inform a decision on whether Article 80(2) should be implemented.

9. **For this reason, we call on you to amend the current Clause 183 to allow for approved not-for-profit bodies to represent unnamed data subjects in data protection infringement complaints.**

10. The Government decided to first review (two years after the Data Protection Bill gets its Royal Assent) how power given to data subjects to designate a not-for-profit body to represent them (Article 80(1)) in their complaints is used. Then they would use this review to provide insight on whether Article 80(2), which allows not-for-profit bodies to represent data subjects without being designated by them, should also be implemented.

11. We have argued previously that this review on a hypothetical power against a separate but complementary power is not going to give any helpful insight into consumer and data protection frameworks.

Review does not tell the whole story

12. The Government's review of the power to designate a body to represent data subjects is likely to consider issues such as how many people decided to raise a complaint this way and what nature of these complaints was.

13. There is a risk that if people do not use the opportunity to designate not-for-profit bodies to represent them, the Government will assume that there is no need for representation.

14. In reality, people not using this opportunity can mean that they either do not wish to have their name associated with a certain complaint or they are not aware of a breach to their data.

Reasons why people do not bring complaints to the ICO

15. People might feel especially reluctant to bring a complaint forward through an organisation under their own name if the information that was leaked about them is sensitive.

16. To illustrate, in 2015 London sexual health clinic sent out the names and email addresses of 780 people who attended the clinic to get HIV tested when a newsletter was issued to clinic patients. Everybody who received the newsletter could see names and email addresses of other recipients. In a case such as this one, it would be likely that people affected by this serious breach of privacy would not want to draw more attention to their association with the data breach due to stigma around HIV. As a result, the issue would end up under-reported and the Information Commissioner's Office [JK1] would have no basis for an investigation into the data breach.

17. In 2013, the LA Gay and Lesbian Community Services Center (LAGLCSC) in the US had their information systems compromised in a cyber attack. The attack revealed names, contact information, medical or healthcare information, dates of birth, credit card information, Social Security numbers and health insurance account numbers of 59,000 clients. Had this attack happened in the UK, it would be understandable if clients of a similar service did not wish to raise this problem with a data protection authority due to the negative impact it could have - revealing their sexual orientation to their family members, friends, employers and acquaintances.

18. Just at the end of 2017, a fertility clinic based in the US notified their clients of a data breach that may have put their personal data at risk. Information leaked about them included names, addresses, phone numbers, dates of birth, email addresses, Social Security numbers, driver's licenses, insurance identification numbers and medical records. A leak of this kind discloses the information of people undergoing fertility

treatment. Making an official complaint would require that affected people admit their privacy has been compromised in this way and could lead to this information being misused further for discriminatory employment practices where an employer might not choose a candidate planning to have a child.

Children and young people cannot complain

19. Young people are often the target of advertising and analysis using their personal data. It has been raised by a number of Peers that apps used by children and young people target them with bespoke advertising and multiple notifications capable of routinely tracking their locations by GPS.

20. A survey in 2015 by the Global Privacy Enforcement Network found that:
    - Only 1 in 3 websites surveyed by the ICO in 2015, had effective controls in place to limit the collection of personal information from children.
    - Only 24% of the sites encouraged parental involvement.

21. However, Open Rights Group has seen no evidence or follow-up from the GPEN report that shows enforcement actions had taken place to improve. With Article 80(2) in place, it would be possible for independent bodies to complain to the ICO and seek remedy to the poor company practices exploiting children's data.

22. Research from consumer group Which? revealed that almost 1 in 5 consumers said they would not know how to claim redress following a data breach, and the same proportion (1 in 5) reporting they would not know who is responsible for helping them when data is lost. These statistics are even more worrying if we take into consideration that these people could be parents of children using privacy invasive apps.

Review of powers

23. The Government's amendment says that they will review the merits of exercising the power under Article 80(2). The merits of implementing the Article are outlined in the examples of people affected above. These cases would not be covered by Article 80(1) and therefore there is an instant merit to implement the other part of Article 80.

24. The Government has created dependency between the two parts of Article 80 when there is none. Article 80(1) and 80(2) complement each other, not depend on each other.

25. For these reasons, we urge you to amend the Bill to include Article 80(2) providing for the possibility of not-for-profit organisations representing unnamed data subjects.

Proposed draft amendment

26. Amendment Clause 183: Representation of data subjects

27. Page 106, line 6, at end insert—

28. “( ) In relation to the processing of personal data to which the GDPR applies, Article 80(2) of the GDPR (representation of data subjects) permits and this Act provides that a body or other organisation which meets the conditions set out in that Article has the right to lodge a complaint, or exercise the rights, independently of a data subject’s mandate, under—
    (a) Article 77(right to lodge a complaint with a supervisory body);
    (b) Article 78 (right to an effective judicial remedy against a supervisory authority); and
    (c) Article 79 (right to an effective judicial remedy against a controller or processor), of the GDPR if it considers that the rights of a data subject under the GDPR have been infringed as a result of the processing.”

29. Page 106, line 13, at end insert –
"() The rights in subsection (2)(a) - (d) may also be exercised by a body or other organisation that meets conditions in subsections (3) and (4) independently of a data subject’s authorisation.”

30. *Member’s explanatory statement*

31. *Enables implementation of Article 80(2) of GDPR and ensures provisions for better empowerment citizen data protection rights and more effective enforcement.*

Manual unstructured personal data

32. Manual unstructured personal data will mainly, but not exclusively, cover handwritten notes, such as minutes of a meeting. Sometimes the official record subsequently circulated diverges from personal recollections and being able to demand the handwritten notes can be important to set the record straight.

33. Clause 21(2) states that the manual unstructured processing of personal data is only subject to the Bill if the controller is a “FOI public authority”. In all other cases, the processing of manual unstructured personal data is not subject to any data protection principle, data subject right or the BIll enforcement regime. This would exclude important situations, such as employment disputes, or discussions with a private provider about the services provided (e.g. health or finances). The loss of sensitive - e.g. health - unstructured data would not be sanctioned at all.

34. Clause 24(2) adds that where the controller is a “FOI public authority” then the manual unstructured personal data are effectively limited to the right of access, correction or erasure. However, if the personal data held by a “FOI public authority” relate to the employment purposes, Clauses 24(3) and 24(4) remove these rights for employees of such public authorities. These are the situations where specifically it would be important to maintain the rights.

35. The DPA currently provides protections for unstructured data and the government has provided no valid reason to change the status quo.

Proposed draft amendment

36. New Clause 21(2A)
37. Page 12, line 25, at end insert -
38. **"**This Chapter also applies to the manual unstructured processing of personal data held by any controller to the extent that it requires compliance with Article 5(1)(f) (principle relating to the security of processing)."

Supplementary amendment

39. Page 14, line 16, Remove **"and (f)"** from Article 5(1)(a) to (c), (e) and (f) (principles relating to processing, other than the accuracy principle)

Member's explanatory statement

40. *This amendment and the supplementary amendment require unstructured personal data to be disposed of securely.*

UK representative for third country processors

41. Under GDPR organisations from outside the EU that process the data of EU citizens must appoint a representative in the territory of the Union that can answer to the ICO and UK courts. The operation of this requirement after Brexit should not reduce the level of protections for people in the UK.

42. The draft Bill modifies the applied GDPR to remove the definition of "representative". As long as the UK remains within the adequacy framework this is not too problematic. However, if the UK falls out of EU adequacy, however unlikely, this removal would bring indefension to UK residents, who would be unable to enforce their rights against a controller fully based overseas.

Proposed draft amendment

43. Schedule 6, page 172, line 26, at end add -
44. "however, this omission is reversed if a controller, based outside the UK or any EU or EEA state but subject to Clause 200, shall appoint a representative in the UK if the UK fails to obtain a determination of adequacy under Article 45 of the GDPR."

Member's explanatory statement

45. *This amendment ensures that a controller based in third countries such as the USA but processing personal data in the UK will need to appoint a representative in the UK; this representative will be actionable by the ICO and other data subjects. Without the amendment, it is difficult to see how the DP Bill can be enforced against a controller based outside the UK.*

Removal of automatic right to legal redress

46. GDPR in Article 78 sets out an automatic right to legal redress if a data protection authority does not respond to a subject complaint within 3 months. The Bill removes this provision without explanation.

Proposed draft amendment:

47. Schedule 6, page 179, line 33, replace -
48. “omit paragraph 2” with “for paragraph 2 substitute --
49. “Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the Commissioner does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.”

Ministers can remove financial penalties for the public sector

50. Penalties are a critical element of the enforcement regime. GDPR allows Member States to set a lower level of fines for public bodies, and even remove them completely. The draft Bill amendment to GDPR in Schedule 6 transfers this power directly to the Secretary of State in absolute form, who could upend the enforcement regime for public sector bodies without the need for consultation. This raises serious questions of accountability and could severely weaken enforcement in the public sector.

Proposed draft amendment

51. Schedule 6, page 180, line 13, replace -
52. Paragraph 56(b) with:

    (a) “omit paragraph 7” (Secretary of State’s powers to set fines for the public sector)

Member’s explanatory statement

53. *This amendment ensures that public sector controllers are subject to penalty notices. If the power in Article 83(7) remains, the UK Secretary of State can follow the Irish and state that the public-sector controllers cannot be fined.*

General identifiers: avoiding a national ID by stealth

54. UK data protection law has long provided a bulwark against the introduction of a national ID system by stealth by providing restrictions on the use of government data as general identifiers that can link various databases. Article 87 of the GDPR sets out restrictions on "national identification numbers", so these identifiers are "used only under appropriate safeguards for the rights and freedoms". The draft Bill removes this Article in the applied GDPR, giving carte blanche for the development of a national ID system without public scrutiny.

Proposed draft amendment

55. Schedule 6, page 180, line 42, remove paragraph 60

Member's explanatory statement

56. *The Government have removed the power in Article 87 for the Secretary of State to protect its own national identifiers (e.g. National Insurance Number; Pupil Identification Number) from being used for unauthorised purposes by controllers. The power is needed to protect such numbers from being used as General Identifiers; the power was in the DPA 1998 and should remain*.

Policy safeguards for processing of some special personal data to be expanded to all in such data under GDPR

57. Schedule 1 of the Draft Bill sets out some special conditions for the processing of certain data that is particularly sensitive: employment, social security, health, and research. These types of data can be processed when it is necessary for reason of substantial public interest. The GDPR Article 9(2)(g) provides a ground for processing of special personal data in the public interest. The article sets out that the Member State law shall "*provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".*

58. However, Article 9(2)(g) is replaced by the text in Schedule 6, paragraph 12(c) which makes no reference to *"suitable and specific measures"*. As a result, the special personal data specified in Schedule 1 is left to be processed in substantial public interest without additional safeguards provided by Article 9 of the GDPR.

Proposed draft amendment

59. Schedule 1, Part 4, page 133, line 34

60. In paragraph 33, replace "Part 1, 2 or 3" with "Article 9(2) of the Applied GDPR, Part 1, 2 or 3"

Member's explanatory statement

61. *Expand the safeguard of a policy document specified in paragraph 36 to the conditions for processing special personal data specified in Article 9(2).*

GDPR safeguards for restrictions of subject rights

62. Article 23 of the GDPR provides for restrictions which may be placed on some specific rights provided by the GDPR (rights specified in Article 12 to 22, 34 and 5). These restrictions are safeguarded in Article 23(2) by providing instances when restrictions can be applied. However, Article 23(2) has not been implemented by the Bill.

63. Article 23(2) ensures transparency is maintained and should be part of the Bill. The Bill should be amended to implement it in terms of a policy document that is made public.

Proposed draft amendment

64. *At page 167, after Schedule 4, insert new Schedule 4A (Safeguards for the processing of personal data subject to a restriction)*

"Schedule 4A (Safeguards for the processing of personal data subject to a restriction)

(1) Each controller that relies on a restriction in Schedules 2, 3 and 4 of this Act shall prepare a policy document that justifies the application of each restriction in terms of:

(a) the purposes of the processing or categories of processing;
(b) the categories of personal data subject to the restriction;
(c) the scope of the restriction;
(d) the safeguards to prevent abuse of the restriction for instance unlawful access to personal data or transfer;
(e) the specification of the controller or categories of controllers that can also rely on the restriction;
(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
(g) the risks to the rights and freedoms of data subjects; and
(h) the right of data subjects in general to be informed about the restriction

(2) The policy document produced under paragraph 1 shall be made public unless the Information Commissioner determines that the document should not be published.

(3) The Information Commissioner shall publish guidance as to what should appear in a policy document referred to in paragraph 1.

(4) Failure to publish a policy document, or the publishing of a policy document that fails to satisfy the requirements of paragraph 1 can be subject to enforcement under Part 6 of this Act."

Member's explanatory statement

65. *Article 23(2) of the GDPR (safeguards for the use of an exemption) has not been implemented by the Bill. The amendment implements this in terms of a policy document that is made public.*