Data Protection Bill, House of Commons Public Bill Committee – Information Commissioner's written evidence

Introduction

1. The Information Commissioner has responsibility in the UK for promoting and enforcing the Data Protection Act 1998 (DPA 98), the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR) and the Privacy and Electronic Communications Regulations 2003, as amended (PECR).

2. She is independent of government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

3. This written evidence updates the Commissioner's previous parliamentary briefings on the Bill.[1] It covers areas where the Commissioner still has outstanding concerns or where there have been developments since she last commented. The Commissioner may submit further evidence in response to amendments or to further questions about the Bill.

Overview

4. The Data Protection Bill puts in place one of the final pieces of much needed data protection reform. It is vital that the Bill reaches the statute book because it introduces strong safeguards for protecting individuals' personal data. Effective, modern data protection laws with robust safeguards are central to securing the public's trust and confidence in the use of personal information within the digital economy, the delivery of public services and the fight against crime.

5. The Commissioner is fully supportive of the Bill and is appreciative of the high level of engagement with the government and Peers during the passage of the Bill through the House of Lords. There are a small number of outstanding issues which, if not resolved, could have a significant impact on her ability to conduct investigations and exercise her powers and functions in an independent and effective way. Her most significant concerns centre on:

    a) The Commissioner's ability to acquire the information she needs to assess whether the law has been broken. (Information notices: clauses 143 and 154)

[1] https://ico.org.uk/about-the-ico/what-we-do/ico-policy-views/

b) The Commissioner's independence when assessing whether processing of personal data by certain public bodies is in compliance with the law. (Framework for Data Processing by Government: clauses 185-188)

c) The breadth and effect of the exemption for defence purposes removing safeguards, individual rights and reducing the Commissioner's powers. (National security and defence exemption: clauses 26-28).

Part 6: Ability to compel compliance with an Information Notice

6. The Commissioner would like the Bill amended to provide a mechanism to require the disclosure of requested information under her Information Notice powers. Failure to do this will have an adverse effect on her investigatory and enforcement powers. The lack of such a mechanism at present is affecting her investigation of current significant cases.

7. Under the current Data Protection Act (DPA 1998), non-compliance with an Information Notice (IN) is a criminal offence, punishable by a fine in the Magistrate's Court. However, the court cannot compel compliance with the Information Notice or issue a disclosure order. This means, that although the data controller can receive a criminal sanction for non-compliance, the Commissioner is still unable to obtain the information she needs for her investigation.

8. This gap in her enforcement powers hasn't caused significant problems up until now, because formal action has largely been centred round security breaches or contraventions of the Privacy and Electronic Communications Regulations. In these cases, she rarely needs to use her information notice powers because the evidence of a contravention is usually clear and in the public domain.

9. Where she has used her enforcement powers against a data controller for contraventions of the data protection principles under the DPA, she has generally found data controllers to be cooperative, because under the current framework financial penalties are reserved only for the most serious contraventions of the law.

10. The Bill removes failure to comply with a notice from being a criminal offence and now provides the Commissioner with only the power to impose a penalty notice (Clauses 143 and 154). This will mean that the Commissioner is still be unable to obtain the information she needs for her investigation.

11. A current investigation into the use of data analytics by political campaigns, particularly during the EU referendum, has shone a light on the gap in her powers, because she has found it necessary to issue a number of INs in an

attempt to obtain the information that is necessary to be able to carry out an effective investigation, and without a power to compel compliance, there is no guarantee of success.

12. In addition, because her power to issue an IN is limited to data controllers, it has not been possible for her officials to obtain information that is relevant to the investigation from uncooperative individuals and witnesses who are not data controllers, which will result in gaps in the investigation and may affect outcomes as it proves impossible to follow essential lines of enquiry.

13. Significant developments in the use of Big Data, Artificial Intelligence and machine learning means that complex investigations such as this will only increase in the future; this coupled with a step change in the regulatory sanctions available to the Commissioner under the GDPR - including an ability to issue substantial fines - means that data controllers are likely to be more reluctant to disclose information as part of an investigation, knowing that the consequences of being found to be in breach will be significant.

14. The new approach in the Bill of failure to comply with an IN no longer being a criminal offence but punishable by a monetary penalty issued by the ICO is likely to be less of a deterrent, as data controllers with deep pockets might be inclined to pay the fine, rather than disclose the information being requested.

15. This is in marked contrast to the approach taken in the Republic of Ireland where many non EU multinational technology companies base their EU operations. The Irish Government's recently published draft data protection legislation makes failure to comply with an information notice issued by the Commissioner a criminal offence carrying a custodial sentence of up to five years imprisonment together with a €250,000 fine. These tougher potential sanctions are more likely to lead to compliance with an IN.

16. The approach in the Bill does not only pale in comparison with our closest EU neighbour, in her previous role as the Information and Privacy Commissioner for British Columbia, the Commissioner had a power to compel the disclosure of documents, records and testimony from data controllers and individuals; and failure to do so was a contempt of court. This was a crucial tool in enabling her to reach a successful outcome to the 'Access Denied' Investigation – which involved the need to compel information from data controllers and individuals; and she continues to believe it is an essential tool for a modern data protection regulator in protecting the rights of citizens in a fast moving digital world.

17. The Commissioner has had constructive conversations with Government about remedying this gap and she is hopeful that a resolution can be reached.

Clause 185: Framework for data processing by Government

18. The Commissioner is concerned that the current provisions will have an adverse effect on perceptions of her independence and ability to take enforcement action against government departments and specified public bodies. These provisions need amending to remove the duty to take account of the Framework when exercising her functions.

19. The Commissioner understands the Government's objective in seeking to provide a clearer legal basis for government departments for their processing activities, particularly around data sharing. However, she believes these provisions are drafted in a way that goes further than this objective and creates the potential for regulatory confusion.

20. The Commissioner remains particularly concerned about the provision that will require her to take the framework guidance into account when considering any questions relevant to her functions. This risks undermining her independence because it gives the impression, even though this is not the Government's intention, that she is not completely free from external influence when exercising her functions as required under Article 52 of the GDPR.

21. The Commissioner considers this provision to be unnecessary because she already takes into account relevant statutory and sectoral guidance when exercising her functions. Should she fail to do so, she could be subject to judicial review and her decision would be scrutinised on any appeal arising from her enforcement action. She appreciates that the revised draft Explanatory Notes attempt to alleviate concerns by emphasising the limited scope of this provision, but this only serves to highlight its unnecessary nature.

22. The Commissioner’s research shows that the public are concerned about who their data is shared with and reflects concerns that they have lost control over how their information is used. It is important that the government’s ambitions to make better use of public sector data and to maximise the use of data analytics and artificial intelligence inspires confidence in those who will be affected. An independent regulator has an important part to play in helping build the public’s trust and confidence in the public sector’s use of data.

23. The Commissioner also has concerns about the scope of the provision and what organisations these provisions are intended to apply to; and the need to ensure the framework guidance doesn't overlap with other statutory codes on data sharing, including her own statutory code of practice on data sharing.

24. The Commissioner considers it would be helpful for the government to publish a draft of the framework guidance during the passage of the Bill to enable parliamentarians and others to judge the extent and likely value of that guidance and how it fits with existing statutory guidance.

25. It will be important to avoid regulatory overlap, especially given how far ranging the definition of data processing is - meaning that it could cover any aspect of data handling within government or other bodies to whom the measure applies.

Clause 26 and 28: National security and defence

26. The Commissioner is concerned about the breadth and effect of the exemption for defence purposes and its potential for removing safeguards and reducing the Commissioner's powers in practice. The government's promised clarifications in the explanatory notes, although welcome, have done little to ease these concerns. The exemption needs adjusting to reduce its potential scope, ensure there is an appropriate threshold for relying upon its provisions and restore the Commissioner's powers to ensure that any reliance on the exemption is appropriate.

27. The Commissioner recognises that there is a need for exemptions in the area of defence, as is the case under the current DPA and acknowledges that defence purposes are excluded from the GDPR. However, in all three of her previous briefings on the Bill for the House of Lords, the Commissioner has raised concerns at the potential for a broad reading of "the purposes of defence" at clause 26, which applies very wide exemptions from various GDPR rights and obligations for national security and defence. She also has serious concerns that clause 26 as drafted would appear to remove processing for defence purposes from regulatory oversight by the Commissioner. The Deputy Counsel to the Joint Committee on Human Rights has also raised concerns about these clauses in her advice to Committee[2].

28. The exemption serves to restrict the Commissioner's powers meaning that in the face of a claim of unwarranted reliance on the clause 26 exemption, the Commissioner would be unable to conduct even the most preliminary of investigations into whether or not the exemption has been correctly applied. Clause 26(2) (e) operates to dis-apply Articles 57(1)(a) and (h) and Article 58 of the [applied] GDPR which provide the Commissioner with her substantive powers to monitor and investigate compliance.

29. Similarly clause 26(2) (f) operates to dis-apply Chapter VIII of the [applied] GDPR which sets out the rights of a data subject, or any organisation

[2] http://www.parliament.uk/documents/joint-committees/human-rights/correspondence/2017-19/Note_Deputy_Counsel_DPBill.pdf

representing data subjects, to complain to the supervisory authority (the Commissioner in the UK).

30. These are significant limitations to the ability of an individual to complain to the Commissioner about their concerns on incorrect reliance upon the exemption and the Commissioner's ability to investigate whether such a wide ranging exemption has been correctly relied upon. The ability of an individual to raise their concerns and the Commissioner's ability to investigate these need restoring.

31. The breadth of the term "defence purposes" was raised during consideration in the House of Lords. Lord Ashton and Baroness Williams in their letter to the Lords of 24 November 2017[3] clarified that the term "defence purposes" was "intended to be limited in both application and scope and would not encompass all processing activities conducted by the Ministry of Defence".

32. They explained that "only where a specific right or obligation is found to be incompatible with a specific processing activity being undertaken for defence purposes can that right or obligation be set aside. The Ministry of Defence will continue to process personal information relating to both military and civilian personnel in a secure and appropriate way, employing relevant safeguards and security in accordance with the principles of the applied GDPR. It is anticipated that standard HR processing functions, such as the recording of leave and management of pay and pension information will not be covered by the exemption."

33. They confirmed that the scope of the definition would be clarified in the explanatory notes to the Bill when they were re-issued on Commons introduction. Although it appears to be the intention of the government to interpret the exemption narrowly, this does not appear to be the effect of the clauses as currently drafted in the Bill, nor the breadth of the interpretation of 'defence purposes' in the in the explanatory notes.

34. The explanatory notes provide a non-exhaustive list of wide-ranging examples of processing activities "which might be considered defence purposes requiring the protection of the exemption". They go on to say:

35. "This is not an exhaustive list, and the application of the exemption should only be considered in specific cases where the fulfilment of a specific data protection right or obligation is found to place the security, capability or effectiveness of UK defence activities at risk."

36. However, wording to this effect does not appear on the face of the Bill. It merely refers to 'defence purposes' and there is no threshold for when it is appropriate to rely on the exemption.

[3] http://data.parliament.uk/DepositedPapers/Files/DEP2017-0720/eCase_07817_-_Peers__DPB.pdf

37. The defence exemption needs to be more focused. Section 26 Freedom of Information Act (FOIA) may provide a helpful example of how this could be achieved. In short:

38. Section 26 provides the public authority with an exemption from the duty to confirm or deny it holds the information but only where this would damage the defence of the British Islands, or the capability, effectiveness, or security of the armed forces. And

39. Section 26 is a qualified exemption. This means that it can only be relied upon where the public interest in maintaining the exemption outweighs the public interest in disclosing the information.

40. Providing greater emphasis on the damage to defence and effectiveness of armed forces would focus the exemption on the areas of specific concern and make it a more proportionate interference with safeguards and individuals rights.

41. Similarly, clause 26 (1) (b) does not set a threshold for when the defence purposes exemption becomes active. This in marked contrast to the Bill's provisions at Schedule 2 relating to immigration and crime and taxation. These include a test of the extent to which compliance with the usual data protection safeguards and individual's rights would be 'likely to prejudice' those matters. This test ensures that dis-applying the data protection safeguards and rights can only take place where there is a real likelihood of prejudice, not the remotest possibility that could be the case however unlikely in practice.

42. Adopting these approaches of being clearer about the defence matters that are of concern and ensuring an appropriate test is in place, would help ensure that the limitation on safeguards and rights are far more proportionate than at present.

Schedule 2: exemption for immigration processing

43. Part 1, paragraph 4 of Schedule 2 introduces a wide exemption in the context of immigration. The provision exempts the 'listed GDPR provisions' for the processing of personal data for either 'the maintenance of effective immigration control' or the 'investigation or detection of activities that would undermine the maintenance of effective immigration control' to the extent that those provisions would be likely to prejudice those purposes.

44. The 'listed GDPR provisions' include information to be provided to data subjects; access to personal data; right to erasure; restriction of processing; and objections to processing. The provisions also exempt requirements for fair and transparent processing. The government amendments agreed at

Lords Report Stage not to include the right to data portability and the right to rectification in this exemption are positive steps.

45. Baroness Williams wrote to Lord Clement-Jones on 23 November 2017[4] explaining the position of the government on this immigration exemption. The Commissioner notes the reassurances that the provision was not a blanket 'carve out' for all immigration matters and would only be used in a targeted and proportionate way to prevent prejudice to the maintenance of effective immigration control.

46. The Commissioner also notes her statement that the Information Commissioner's Office will still have oversight of all processing for immigration purposes and the government is not seeking to remove a data subject's right of redress. The government's statement also makes clear that the exemption can only be invoked to the extent that compliance with data subject's rights is likely to prejudice the maintenance of effective immigration control or the investigation or detection of activities that would undermine the maintenance of such control.

47. The Commissioner notes that the term 'maintenance of effective immigration control' is wide and would presumably apply to private organisations carrying out functions for the state – such as private sector organisations running immigration detention centres. It could also draw in organisations who are processing personal data for the purposes of checking right to work status of individuals

48. The Commissioner is concerned that this exemption is not interpreted in a way that is inconsistent with the Minister's assurances. She will take an interest in how this new exemption operates in practice and is applied in a way that is transparent and fair to individuals.

Clause 183: Representation of data subjects

49. The Commissioner has noted the continued debate around the government's decision not to make provision for GDPR Article 80(2) in the Bill – which would allow representative bodies to take action on behalf of data subjects without requiring their specific mandate to do so. This has sometimes been described as a *super-complaint* type procedure.

50. The Commissioner continues to support the derogation at Article 80(2) being exercised to provide representative bodies with this right of action. She welcomes the government's commitment to amend the Bill to provide for a review of the effectiveness of Clause 183 - including looking again at Article 80(2) - and to provide the power for the government to implement its conclusions.

[4] http://data.parliament.uk/DepositedPapers/Files/DEP2017-0730/2017.11.23_Letter_from_Baroness_Williams_to_Lord_Clement-Jones.pdf

51. She is pleased that many parliamentarians have spoken in support of the inclusion of a provision to exercise the derogation available to the UK at Article 80(2), in terms of both recent high-profile data breaches, and also the benefits of enabling representative bodies to hold data controllers and data processors to account when they have not dealt with personal data in accordance with the law.

52. As was highlighted in debate, there are circumstances where data subjects may not necessarily be aware of what data about them is held by organisations, and more importantly what is being done with it. In such instances data subjects could not be expected to know whether and how they could exercise their rights under data protection law. Furthermore, in the context of wider discussion of the Bill and children's rights, the relevance of this point is of particular importance where young and vulnerable data subjects are involved – these groups being less likely to have the means and capability to exercise their rights on their own behalf.

Clause 121: Code on personal data of national significance

53. This clause would require the Commissioner to produce a code of practice on "personal data of national significance" which includes setting out best practice in relation to economic or societal value of release of personal data to third parties.

54. The clause raises important issues and these may become more pressing in future as technology develops and individuals become more aware of where their data is held and how it is put to particular uses. However, the Commissioner considers that she is not best placed to advise on 'value for money' and securing financial benefits from the sharing of such personal data with third parties for the purposes of processing or developing associated software. These are matters far removed from her core information rights safeguarding function.

55. There are others in government or the wider public sector, whose core function is to drive value added from national assets (including information datasets), and may be a more natural home for providing this best practice advice.

The special purposes

56. The Commissioner has noted the extensive debates about journalism during the Bill's progress through the House of Lords. She was disappointed to note that since the Bill was originally drafted, the then clause 164(3)(c) was removed by government amendment. Without this provision the Commissioner cannot make a determination where she agreed that processing was for the special purposes and with a view to publication of

journalistic, academic, artistic or literary material previously unpublished by the controller but the application for the GDPR's provisions would not be incompatible with those special purposes. This means that it would be possible for privacy rights to be overridden even where there was no need to do this to protect freedom of expression including the special purposes.

57. This clause did not provide the Commissioner with any far reaching new powers that would affect the processing of data for the special purposes as was argued by some during Lords Committee Stage. It did not create a power for the Commissioner to prevent publication. It served to cure a drafting defect in the existing data protection regime that has resulted in individuals being unable to rely on their data subject rights even though these rights would not be incompatible with the special purposes.

58. The Commissioner's existing guidance entitled 'Data Protection and Journalism: a guide for the media'[5], explains the significant additional checks and balances when the Commissioner is contemplating action in relation to the special purposes. These include having to apply to a court for leave to serve enforcement and penalty notices. The court must be satisfied that the Commissioner has reason to suspect a breach of substantial public importance before granting such an application and that the intended recipient has been given notice to enable them to contest the application before it is granted. These important additional special purposes safeguards are also taken forward in clause 151 (enforcement notices: restrictions) and clauses 155 (penalty notices: restrictions) of the Bill.

59. Examples of where this current drafting defect has caused difficulties include a number of the cases involving individuals pursuing their subject access rights to request a copy of previously published material, such as photographs, where the media bodies concerned argued that it may be published again so it is retained with a view to future publication. These requests were denied and the Commissioner had no way of making a determination that giving access would not be incompatible with the special purposes. This defect also means that individuals are prejudiced when trying to take their own legal action to enforce their rights, as any proceedings would be stayed by a court until the Commissioner was able to make such a determination. This clause would have resolved the drafting defect that causes that 'Catch 22' situation with no redress for individuals and ensured that the new legislation does not perpetuate this anomaly.

Information Commissioner
7 March 2018

[5] https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf