Data Protection Bill, House of Commons Public Bill Committee – Information Commissioner's further 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 submission to the Public Bill Committee on 8 March 2018.[1] The Commissioner would like to draw the Committee's attention to two areas of concern: the agreed amendment to Clause 8 on democratic engagement; and deficiencies in her enforcement powers in relation to data protection impact assessments (DPIAs) in the area of law enforcement.

Activity that supports or promotes democratic engagement (agreed amendment to Clause 8)

4. The Commissioner has concerns about the government amendment agreed in Committee on 13 March 2018 which added democratic engagement activity to the list in Clause 8 of examples of processing activities that could be undertaken on the grounds of lawfulness of processing in the public interest.

5. The amendment added point (e) "an activity that supports or promotes democratic engagement" to Clause 8. This clause references lawfulness of processing in Article 6 (1) (e) of the GDPR which sets out processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority.

6. Margot James MP, in presenting the amendment in Committee, said the term had been deliberately chosen with the intention of covering "a range of activities carried out with a view to encouraging the general public to get involved in the exercise of their democratic rights". She said it could include communicating with electors, campaigning activities, supporting candidates and elected representatives, casework, surveys and opinion gathering and

[1] Written Evidence: Information Commissioner's Office (DPB05)

fundraising to support any of those activities. Any processing of personal data in connection with those activities would have to be necessary for their purpose and have a legal basis. The explanatory notes would include examples, to aid interpretation.

7. The Minister said it was not intended to create new exemptions from the data protection legislation. "It is intended to provide greater clarity. It is also independent of any particular technology, given that in a short time we have moved from physical post to email, Twitter, text messages, WhatsApp, Facebook and so forth."

8. Whilst the Commissioner understands the importance of the public interest in enabling democratic activity, she has a number of concerns about the amendment. Most significantly she considers that consent or "legitimate interests" under article 6 of the GDPR are the more appropriate lawful bases for such processing. The legitimate interest basis enables the balancing test of whether such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This balancing test is important to ensure that some organisations do not use a broad legal basis to legitimise some of the campaigning techniques the Commissioner's office is looking at in her investigation into data analytics for political purposes.

9. Having considered Recital 45 of the GDPR, the Commissioner considers that not all democratic activities would be covered by Article 6 (1) (e). It is likely to be restricted to activities such as those covered by electoral law, for example sending mail outs allowed to each voter. Unlike the democratic engagement, the other activities listed in Clause 8 do have a broad legal basis, for example if necessary for the exercise of a function conferred by enactment, functions of Parliament or the administration of justice.

10. The very wide democratic engagement provision also contrasts with the processing of special category data (political opinions) in the relevant Article 9 legal basis in the Bill as drafted (and the current DPA 1998 Schedule 3 condition) which are only able to be used by registered political parties rather than by any data controller. Other campaigners or private sector organisations have to rely on consent unless, for example, electoral law allows them access to the full electoral register in advance of a referendum.

11. It is recognised that political parties have concerns about a lack of clarity on whether certain activities would be lawful under the GDPR. The Information Commissioner would be very willing to help clarify in her guidance that activity that supports or promotes democratic engagement can be a legitimate interest.

12. Engaging voters is important in a healthy democracy, and in order to do that, political parties, referendum campaigners and candidates will campaign using a variety of communication methods. However, they must comply with

the law when doing so; this includes the handling of the personal data that they collect and hold. The Committee should be aware that the Privacy and Electronic Communications Regulations (PECR) will also apply to electronic communications to promote a political view in order to gain support at the ballot box, or otherwise influence an individual, this will include its requirements for consent.

Enforcement of data protection impact assessments relating to law enforcement provisions (Clause 148)

13. The Commissioner considers that the Bill should be amended to ensure that she has the same ability to impose corrective measures, where necessary, when a Data Protection Impact Assessment (DPIA) reveals that processing is of high risk to individuals and where there are no measures to mitigate that risk, in relation to law enforcement processing as she has for other processing. This different approach is not justified and may lead to adverse consequences in an important area affecting individuals.

14. Assessing data protection and privacy risk before processing takes place is important for ensuring a privacy by design approach. Data protection safeguards can then be built in from the outset and designed into systems. The Commissioner has long advocated this and developed tools, like her Privacy Impact Assessment code of practice, to help organisations. Both the GDPR and Law Enforcement provisions within Part 3 of the DP Bill now requires these types of assessment to be undertaken where there is a high risk to the rights and freedoms of individuals. They also provide for requirements to consult the Commissioner where such a high risk is present but measures cannot be put in place to mitigate these. They also provide requirements for the Commissioner to use her corrective powers in relation to GDPR but the way the Bill is drafted these corrective powers will not be available in relation to concerns arising from a DPIA involving law enforcement processing. Nor are there any powers available to ensure that the Information Commissioner can take action if a DPIA for law enforcement processing is not carried out when required.

15. This anomaly is not just a small procedural difference, it is matter of significant concern. It is particularly likely that law enforcement processing, by its very nature, may engage this prior consultation duty. The Commissioner has had to take action in relation to such processing where no or ineffective PIAs have been undertaken that failed to properly identify and address privacy risk and the processing was commenced. The Commissioner's enforcement case that tackled the unwarranted encircling of the small town of Royston with automatic number plate recognition cameras is a case in point. Having the ability to issue corrective measures based upon the DPIA or indeed requiring a DPIA to be undertaken when it should have been, is an important measure which is missing in relation to law enforcement processing and the Commissioner has raised her concerns with

the government and suggested drafting solutions that would remedy the issue. Amending clause 148 (2) to ensure that the requirements at clause 65 are covered would be a straightforward solution.

Information Commissioner

19 March 2018