Annex II

Data Protection Bill, House of Lords Report Stage – Information Commissioner's briefing

1. This annex provides an update to the Information Commissioner's previous briefings for the House of Lords Second Reading and Committee Stages. It responds to some of the points raised during the detailed Committee Stage scrutiny and expands upon those issues that still remain of interest or concern to the Commissioner as the Bill proceeds on to Report Stage.

Help for organisations to prepare for data protection reform

2. The Commissioner is providing a package of wide-ranging advice and guidance to help organisations in all sectors prepare for data protection reform. She published a new Guide to the GDPR[1] on 21 November 2017 which at the time of writing has attracted in excess of 200,000 unique page views.

3. The guide explains the provisions of the GDPR to help organisations comply with its requirements. It is aimed at those who have day-to-day responsibility for data protection in their organisation. It is a living document that will expand as more detailed guidance on specific areas becomes available in advance of May 2018.

4. ICO guidance is designed to engage a range of different audiences and address their needs, from "at a glance" key information summaries to more substantive detailed guidance.

5. As the UK's supervisory authority for data protection, the Information Commissioner is also actively engaged with representatives of data protection authorities from all EU member states on the drafting and issuing collective guidance. This guidance is produced under the auspices of the Article 29 Working Party. Since the Commissioner's last briefing annex for peers, the Article 29 Working Party has concluded consultations on draft

[1] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

guidance on data breach notifications, administrative fines, and automated decision making and profiling. It has also recently adopted guidelines on both transparency and consent. Once these are published there will be a short period of public consultation before final adoption.

6. The ICO data protection self-assessment toolkit, launched in 2016, is an online resource to support small organisations in improving their information rights compliance. The toolkit has been well received by data controllers in the UK and was also recently acknowledged internationally[2]. Since the Commissioner's last briefing annex, the toolkit has been supplemented with additional material specific to the new legislative changes.

7. This support is in addition to the ICO's new dedicated telephone service aimed at helping small businesses and charities prepare for data protection reform. This was launched on 1 November and is distinct from our existing public helpline, which handled over 190,000 calls last year. To date the small business helpline has responded to over 4,000 calls for assistance.

Clause 175: Framework for Data Processing by Government

8. Clause 175 has been added to the Bill by government amendment and provides for a guidance document to be issued by the Secretary of State on data processing by government departments and other public bodies. Clauses 176 to 178 have also been added, to further address the effect of the framework and how it will be approved and published. The Commissioner understands that these amendments were introduced to provide government departments with a clearer legal basis for their processing activities, especially around data sharing.

9. The Commissioner understands the need for government departments and public bodies to be clear about their legal basis for undertaking their functions and this is particularly true when processing personal data. However the provisions as drafted appear to go beyond this limited ambition and create different risks that must also be considered. She has made clear her concerns to government and these are set out below.

10. In addition to the framework applying to processing of personal data by government departments, Clause 175(1)(b) provides for regulations to be made specifying persons with functions of a public nature whose processing would also be covered by the scope of the framework. This wording does not appear constrained to just public bodies who may have concerns about their legal basis, but to others who may be able to act privately but nevertheless undertake some limited functions of a public nature. These provisions should just address those public bodies where there is a need for greater clarity on

[2] https://icdppc.org/wp-content/uploads/2017/09/ICDPPC-Awards-Winners-list.pdf

their legal basis for processing. This regulation-making power seems unnecessarily wide to achieve the government's objective of addressing data processing primarily within government departments and there should be a clearer, more focussed provision setting out the other bodies to which the requirement may be applied.

11. The inclusion of a requirement on the Secretary of State to consult the Commissioner when drawing up the framework guidance is welcome but she remains concerned about the potential for regulatory confusion. There are already a number of statutory codes of practice touching on processing for sharing data especially by public bodies. These include codes of practice that are being developed by the Secretary of State under powers in the Digital Economy Act 2017[3] and the Information Commissioner's own existing statutory code of practice on data sharing (as taken forward under Clause 119 of the Bill). There is an obvious risk of unnecessary and potentially confusing regulatory overlap if the framework guidance also covers these areas.

12. It will be important to ensure that any guidance produced by the Secretary of State is consistent with this existing body of statutory guidance. The framework guidance deals with data processing. The definition of this is very wide and could cover any aspect of data handling within government or other bodies to whom the measure is applied. A draft of the likely framework guidance should be published during the passage of the Bill to allow parliamentarians and others to judge the extent and likely value of that guidance and how it fits with existing statutory guidance.

13. The Commissioner's most significant concerns centre on Clause 178(5). This puts a duty on the Commissioner to take the Secretary of State's framework guidance into account when considering any question relevant to her functions. Whilst she understands the relevance of considering any guidance about the legal basis of government functions the provision runs a real risk of creating the impression that the Commissioner will not enjoy the full independence of action and freedom from external influence when deciding how to exercise her full range of functions as required by Article 52 of the GDPR.

14. Introducing a statutory requirement on the Commissioner to take the Secretary of State's framework guidance into account is not required as the Commissioner already takes into account relevant statutory and sectoral guidance when exercising her functions. Should she fail to do so she would be open to judicial review and this failure could also be scrutinised on appeal arising from her enforcement action.

[3] https://www.gov.uk/government/consultations/digital-economy-act-part-5-data-sharing-codes-and-regulations

15. For example, the Commissioner takes into account sectoral guidance produced by the police service when examining issues related to the processing of personal data by that sector. Similarly, when she is considering matters relating to the processing of personal data acquired by surveillance cameras operated by relevant authorities under the Protection of Freedoms Act 2012 she takes into account the provisions of the Secretary of State's Surveillance Camera Code of Practice issued under that legislation. The Commissioner would also take into account the Ministerial Code of Data Matching Practice issued under Schedule 9 the Local Audit and Accountability Act 2014 when examining question around data matching by relevant authorities. The same will be true of codes of practice that the Secretary of State issues under Part 5 of the Digital Economy Act 2017. There are no statutory requirements to do this under any of these pieces of legislation and including a provision relating to the Secretary of State's framework guidance is similarly unnecessary under this Bill.

16. Requiring the Commissioner to take the Secretary of State's framework guidance into account is unnecessary in practice and in the context of other similar statutory guidance. If greater assurance is required that framework guidance would be taken into account where relevant then the Commissioner will make clear her approach in her guidance about regulatory action that she is required to produce under Clause 153 of the Bill.

Schedule 2: Exemption for immigration processing

17. Part 1 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.

18. The 'listed GDPR provisions' include information to be provided to data subjects, access to personal data, right to rectification, right to erasure, restriction of processing, right to data portability and objections to processing. The provisions also exempt requirements for fair and transparent processing.

19. As the exemption relates to the purpose for processing, it 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 for example. The term 'maintenance of effective immigration control' is wide and, although reliance on the exemption is conditional on the 'likely to prejudice' test, this

should be a more focussed provision with reference to specific statutory immigration functions.

20. The majority of data protection complaints to the Information Commissioner about the Home Office relate to requests for access to personal data to UK Visas and Immigration, mostly by solicitors acting on behalf of those seeking asylum. This exemption could potentially render personal data unobtainable to the data subject and this could be detrimental to individuals who are appealing asylum decisions for example. If the exemption is applied, individuals will not be able to access their personal data to identify any factual inaccuracies and it will mean that the system lacks transparency and is fundamentally unfair.

21. The current Data Protection Act 1998 (DPA 98) does not provide an exemption in the context of immigration. It is accepted that an exemption should be available in limited circumstances such as, for example, so as not to prejudice the investigation of an individual who has overstayed their permitted term in the UK but this could be limited in the Bill to only restrict access to personal data rather than all the other 'GDPR provisions' which would be exempted.

Clause 24: National security and defence

22. In her previous briefing for Second Reading, the Commissioner had raised her concern at the potential for a broad reading of "the purposes of defence" at Clause 24, which applies exemptions from various GDPR rights and obligations for national security and defence. She had sought assurance from government that the more narrow definition of processing for defence purposes would be clarified so that the exemption is not applied to a wider range of processing than that to which it applies in the DPA 98.

23. The Commissioner welcomes the commitment by Lord Ashton and Baroness Williams in their letter[4] to peers of 24 November 2017 – in which they confirm that this scope of the definition will be clarified in the explanatory notes to the Bill when they are updated.

24. The Commissioner will remain alert to this issue and be keen to ensure that the refreshed explanatory notes to this clause are consistent with the ministerial commitment.

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

Clause 41: Overview and scope (of data subject rights)

25. Clauses 41(3) and (4) provide for restrictions to data subject rights in relation to the processing of 'relevant personal data' contained in documents relating to criminal investigations or prosecution proceedings that are created by or on behalf of a court or other judicial authority.

26. Whilst the Commissioner recognises there are other alternative routes to obtain information such as through the disclosure provisions in the Criminal Procedure and Investigations Act 1996, Clause 41, as drafted, appears to restrict not just access rights but appears to restrict a number of rights such as the right to rectification, right to erasure and restriction of processing in relation to a criminal investigation.

27. The Commissioner understands that the intention with this clause is to provide exemptions in relation to personal data processed by the court or judicial authority as part of the criminal proceedings, which would include judges' notes, and not to the whole of the criminal investigation. The wording of the clause includes the words 'criminal investigation' and 'investigation'. This seems to go beyond the government's policy intent.

28. The explanatory notes could clarify how the exemption should be applied in practice. Removing the words 'criminal investigation' and 'investigation' would allay concerns about interpretation of this provision so that it is limited in scope as intended. The wording in Clause 41(3) would then properly reflect the government's intent if it is redrafted to say 'But sections 42 to 46 do not apply in relation to the processing of relevant personal data in the course of criminal proceedings including proceedings for the purpose of executing a criminal penalty.' Clause 41(4) could then be amended to remove the word 'investigation' so it would read 'In subsection (3) 'relevant personal data' means personal data contained in a judicial decision or in other documents relating to the proceedings which are created by or on behalf of a court of other judicial authority'.

Part 4: Intelligence services processing

29. Part 4 of the Bill applies to processing by the intelligence services - defined at Clause 80(2) as the security service, the secret intelligence service and GCHQ. This would also cover emanations of these bodies such as the National Cyber Security Centre. The Commissioner has previously noted the restrictions in Part 4 in terms of specific regulatory obligations and oversight. Central to the reliance on the restrictions is the issuing of a certificate to be signed by a Minister of the Crown (Clauses 25 and 109). Whilst there may be instances where the revelation of such a certificate could itself affect national security, the Commissioner has stated that there should be a presumption of placing these in the public domain where this would not be the case. Similarly there was no requirement for the

Commissioner to be notified when a certificate is issued. This is in contrast to the Investigatory Powers Act 2016 where the Commissioner is to be informed when the Secretary of State issues a retention notice to a Communications Service Provider. The Commissioner took the view that adopting a similar provision in relation to national security certificates may provide a further safeguard to help inspire public confidence in the extent of regulatory oversight.

30. Baroness Williams said[5] during the Committee Stage debate that national security certificates are public in nature and that the government will explore how they can make information about national security certificates issued under the Bill more accessible in future. This commitment has resulted in the tabling of an amendment after Clause 125 on records of national security certificates. This provides for the Commissioner to be informed of all such certificates and requires her to publish these unless a Minister makes a determination otherwise such as where doing so itself would be against the interests of national security. This is very welcome as it should improve regulatory scrutiny and foster greater public trust and confidence in the use of national security certificate process.

The special purposes

31. The Commissioner is disappointed to note that Clause 164(3)(c) has been tabled for removal by government amendment. As explained at paragraph 26 in the earlier annex to this briefing, without this provision the Commissioner could not 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.

32. This clause does not provide the Commissioner with any far reaching new powers that would affect the processing of data for the special purposes as has been argued by some during Committee Stage. It does not create a power for the Commissioner to prevent publication. It serves 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.

33. The Commissioner's existing guidance entitled 'Data Protection and Journalism: a guide for the media'[6], explains the significant additional checks and balances when the Commissioner is contemplating action in

[5] House of Lords Hansard, 15 November 2017, Volume 785
[6] https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf

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 145 (enforcement notices) and clause 149 (penalty notices) of the Bill.

34. 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.

Protection of children's data

35. The issue of children's data and their rights under the Bill was the subject of detailed and wide-ranging debate at Committee Stage, and the Commissioner welcomes the widespread recognition of the importance of getting this area of data protection right. Media and public awareness of this issue is increasing, with recent reports citing the finding that underage use of social media sites is growing. It is clear that the protection of children's data is an important component of how children and young people interact with the digital world. The Commissioner recognises that a variety of expertise will need to be drawn on to tackle this issue effectively, and a coordinated approach will be required from government, the public sector, the private sector, and society as a whole.

36. The Commissioner notes that during the debate, the proposal was made that organisations be required to commit to minimum standards of age appropriate design where they provide online services to children and young people. In response the Government has introduced an amendment requiring the Commissioner to produce a code of practice on age appropriate design. The Commissioner welcomes this and feels that this requirement furthers the concept of data protection by design, which is a key feature of GDPR. However it is important that there is clarity on the contents of the code and in particular the matters to be included in guidance from the Secretary of State to which the Commissioner must have regard when drawing up her code. It would be preferable if the areas to be covered

by such guidance were included on the face of the Bill. In furtherance of the Commissioner's commitment to the wider debate on children's and digital issues, she will be publishing a consultation on draft ICO guidance relating to children's data and the GDPR in December 2017.

Representation of data subjects

37. 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. 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.

38. As was highlighted in the Committee Stage 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. The Commissioner continues to support the derogation at Article 80(2) being exercised to provide representative bodies with this right of action.

Data ethics

39. Concerns about addressing data ethics were voiced during Committee Stage. The Commissioner is already significantly engaged with the topic of data ethics and data protection is a key component of ethical considerations. She recognises that this is an important area that can go beyond the processing of personal data within her own statutory remit and she has been involved in discussions with interested parties, including government, on this developing area. In particular there is a need for greater foresight into the long term implications of technologies such as artificial intelligence. She welcomes the government's announcement in the Autumn Budget of the creation of a Centre for Data Ethics and Innovation. She looks forward to working with the new body as it develops its role, especially on areas around the impact of technologies like artificial intelligence and machine learning on individuals and society.