Annex

Data Protection Bill, House of Lords Committee stage – Information Commissioner's briefing

1. This annex provides an update to the Information Commissioner's briefing for the Lords Second Reading. It responds to some of the points raised during the Second Reading Debate and to questions made directly to the Information Commissioner's Office.

Help for small businesses to prepare for data protection reform

2. The Commissioner has announced the launch of a dedicated telephone service aimed at helping small businesses prepare for data protection reform. The phone service will add to a package of tools and resources already available for organisations getting ready for the General Data Protection Regulation (GDPR) which comes into effect on 25 May 2018. The new service will go live on 1 November 2017 and will be based around the ICO's existing public helpline, which handled around 190,000 calls last year.

3. The Information Commissioner's Office (ICO) has also announced plans to simplify its popular "12 steps to take now" graphic in response to calls from small and micro businesses that they need access to targeted information about how to prepare for the GDPR.

4. In addition the ICO is revising its simple-to-use SME toolkit, a resource used by around 9,000 businesses a month since January 2016, into a GDPR checklist that will allow businesses themselves to identify gaps in their own preparation for the new law.

5. This new package of help for small businesses builds on the advice and information that is available on the dedicated section of the ICO's website which includes guidance on the GDPR and the practical steps organisations

can take to prepare for data protection reform [1]. The Commissioner is committed to preparing stakeholders in all sectors for the transition to the new regulatory regime.

Clause 24: Defence exemption

Background

6. Part 2, Chapter 3 of the Bill covers other general processing in the course of activities outside the scope of European Union law.

7. Clauses 24 to 26 create an exemption from certain provisions in this applied GDPR scheme and in Parts 5, 6 and 7 of the Bill if that exemption is required for the purpose of safeguarding national security or for defence purposes. The provisions from which there is an exemption are listed in subsection (2) of Clause 24 and include most of the data protection principles, the rights of data subjects, certain obligations on data controllers and processors, and various enforcement provisions.

Issue

8. The explanatory notes say this exemption is similar to the provision in section 28 of DPA 98 which provides for exemptions. However the existing similar exemption at section 28 of the DPA 98 is confined to just national security so Clause 24 extends this parallel provision to defence. The DPA 98 includes a narrower armed forces exemption in Schedule 7 - Miscellaneous exemptions:

> *2. Personal data are exempt from the subject information provisions in any case to the extent to which the application of those provisions would be likely to prejudice the combat effectiveness of any of the armed forces of the Crown.*

9. The wording for the defence exemption in Clauses 24 and 26 is for processing for the "purposes of defence" and appears to be widely drawn compared to the more specific exemption in the DPA 98 of "likely to prejudice combat effectiveness of the armed forces".

10. We understand from the government that "the purposes of defence" would not be a catch-all term covering everything the Ministry of Defence (MOD) does but it would be more narrowly focussed in its application. We also understand that the MOD seeks to maintain the status quo under the DPA and does not intend to further restrict data subject or other rights other than the rights and obligations listed and where necessary for the purposes of National Security or defence (Clauses 24 and 26). We also understand

[1] ICO website section on data protection reform https://ico.org.uk/for-organisations/data-protection-reform/

that the certification procedure (Clause 25) is not intended to apply to the defence purposes exemption, only to national security.

11. Understanding the context and operation of this exemption in practice will be important and in particular the extent to which the processing of personal data for defence purposes would be outside the scope of the GDPR and potentially subject to these provisions: for example, would the processing of civilian personnel records by a body that has defence responsibilities be outside the scope of GDPR. This means the scope of this new exemption for processing "for the purposes of defence" is likely to be open to interpretation in practice and confirmation from government of its more limited focus will be important.

National security and intelligence services

Background

12. Part 4 applies to processing by the intelligence services (defined at clause 80(2) as the security service [MI5], the secret intelligence service [MI6] and GCHQ).

13. This is all processing undertaken by the bodies themselves, not simply processing undertaken for the purposes of safeguarding national security (or similar). Part 4 therefore departs from parts 2 and 3 in not taking a purposive approach to the processing.

14. The provisions themselves derive from Council of Europe Convention 108[2] rather than GDPR or the Law Enforcement Directive (LED). Convention 108 is an internationally recognised standard to which the UK adheres and has done so since our first generation of data protection law in 1984. Convention 108 applies to the activities of the intelligence services unlike the other two international legal instruments. Although there are variations in the different instruments, it is important that an effective data protection regime applies in practice and there is scope in certain areas for going beyond the requirements of Convention 108.

Issues

15. **Restrictions –** There is an exemption at Clause 108, excluding many of the provisions of Part 4 where such exemption is required for the purposes of safeguarding national security. Though notably, and in contrast to the equivalent exemption at section 28 of the current Data Protection Act 1998, the intelligence services will need to ensure that the processing is fair, lawful, and meets a suitable condition for processing from Schedule 9 and/or

[2] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

Schedule 10 of the Data Protection Bill. There is a similar national security exemption at Clause 24 allied to the defence exemption mentioned above.

16. This exemption also removes or restricts specified regulatory obligations and supervisory powers where the processing is done by the intelligence services and this is required for the purpose of safeguarding national security. These are:

    - the requirement to communicate a personal data breach to the Commissioner;
    - the power of the Commissioner to inspect personal data to carry out an international obligation;
    - the Commissioner's general powers to monitor and enforce Part 4, and conduct investigations on the application of Part 4;
    - various powers associated with the Commissioner's ability to notify, warn or reprimand, in respect of processing;
    - the Commissioner's powers of enforcement (information, assessment and enforcement notices) and associated powers of entry and inspection (including the issuing of warrants);
    - the Commissioner's prosecuting powers in relation to the specific offences of unlawful obtaining of personal data, re-identification of de-identified data, and alteration of personal data to prevent disclosure;
    - the Commissioner's powers in relation to the processing of personal data for the special purposes (artistic, literary and academic purposes and the purpose of journalism).

17. These measures impose limitations on the Commissioner's powers to satisfy herself that the obligations under Part 4 are being observed, or that the residual obligations to process data fairly, lawfully and under a suitable Schedule 9 or Schedule 10 condition remain met.

18. The Commissioner recognises that there is a more complex system of regulatory oversight for the intelligence services. But the Commissioner is concerned to ensure that these restrictions do not result in a very limited requirement to comply with the regulatory safeguards in Part 4 in practice.

19. Central to the reliance on these restrictions is the issuing of a certificate to be signed by a Minister of the Crown (Clauses 25 and 109). There may be instances where the revelation of such a certificate could itself affect national security, but there should be a presumption of placing these in the public domain where this would not be the case. Similarly there is no requirement for the Commissioner to be notified when a certificate is issued. Under the Investigatory Powers Act 2016 the Commissioner is to be informed when the Secretary of State issues a retention notice to a Communications Service Provider. Adopting a similar provision in relation to

national security certificates may provide a further safeguard to help inspire public confidence in regulatory oversight.

20. **Rights of data subjects –** The rights of the data subject in Part 4 are more limited than they are under either Part 2 (GDPR and other general processing) or Part 3 of the Bill (the law enforcement provisions, giving effect to the LED).
21. Some of the differences are:-

    - Right to information - information about the processing which needs to be provided to data subjects is less comprehensive under Part 4.
    - Right to access - there is a fee for access rights and, as part of the information to be provided to a data subject, there is no requirement to inform the data subject of their right to object or their right not to be subject to automated decision-making.
    - The right to rectification and erasure (this is bundled together as one right unlike GDPR) is only exercisable via the courts, as is the right to object to processing. There is no separate right to restriction though provisions are captured under the right to rectification/erasure.

22. The intelligence services process personal data about data subjects which may be of less security sensitivity than others. These could include some employees and contractors who will have more limited rights than those provided for in Part 2.

23. **Other regulatory safeguards –** There are also other limitations that Part 4 of the Bill does not require. This includes the appointment of a Data Protection Officer. Establishing the requirement to have such a person in place may also add to public confidence in the system of internal controls. Similarly, including a comparable requirement to carry out Data Protection Impact Assessments as required under Parts 2 and 3 of the Bill may also help foster confidence in the strength of internal controls around the acquisition and use of personal data.

The Special Purposes

Background

24. Article 85(1) GDPR acknowledges that freedom of expression is a fundamental right along with the right to data protection. It affirms the special weight that should be given to freedom of expression including journalistic purposes. Member States are obliged to reconcile these rights including the processing of personal data for journalistic purposes and for academic, artistic or literary expression. These are defined as the 'special purposes' in the Bill. Paragraph 24 in Part 5 of Schedule 2 of the Bill sets out

the exemption from the GDPR's provisions. Where personal data is processed for the special purposes, controllers will only be obliged to comply with data protection obligations to the extent that they are not incompatible with (i.e. they do not amount to an unjustified interference with) the special purposes.

Issue

25. The Commissioner's general approach has been that the key elements of the DPA 98 should be replicated. For the most part these existing provisions have proved to be a balanced approach to reconciling these rights but in response to the Government's call for views we requested the Government to make a necessary technical change to the ICO's ability to make a determination on the processing of personal data for individuals. This has been reflected in Clause 164(3)(c) which is part of the additional arrangements in place to reflect the importance of processing or the special purposes.

26. 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. This would also impair the operation of Clause 166 as it could also have the effect that proceedings brought by the data controller in the courts will be stayed indefinitely as the Commissioner is unable to make a determination of incompatibility that enables the court to recommence the proceedings.

Protection of children's data

Background

27. The Commissioner recognises the wide range of views expressed in the Second Reading debate of the Data Protection Bill on how best to protect children using the internet and the use of their data. She welcomes the debate on the issue of children's privacy, including how legislation can play a part in empowering and protecting children. There are wider social and cultural issues at play and ethical considerations are also important.

28. These are challenging issues. Data protection is only one part of a wider social issue about how children grow up, interact and express themselves. The use of big data, artificial intelligence and machine learning also has significant implications for privacy and data protection and the associated

rights of individuals. Many data protection concepts can be seen as components of ethical decision-making. The Commissioner wants to ensure that privacy and data protection considerations are integral to big data analytics and that includes the processing of children's data.

29. The Commissioner is keen to work in partnership with others with an interest and expertise in this area. She also supports many of the conclusions of the Children's Commissioner for England in her report Growing Up Digital[3].

Issues

30. **Children's privacy –** The ICO has started a consultation process, including roundtables, to obtain stakeholder feedback on children's privacy but it is a complex area with many difficult issues to consider. We are about to consult more widely and are keen for input from a wide range of stakeholders on some of the more challenging issues. We shall also be responding to the government's green paper "The Internet Safety Strategy".[4]

31. **Clause 8: Child's consent in relation to information society services –** The Bill provides that the age of consent of children using information society services should be 13 years. Under the GDPR a child under the age of 16 cannot give valid consent to the processing of their personal data for the provision of the service, unless the law of their Member State provides a lower age (to be no lower than 13). The Commissioner's submission to the House of Lords Select Committee on Communications' Inquiry into Children and the Internet[5] makes clear that, on balance, the Commissioner favours an approach where even quite young children can access appropriate online services without the consent of a parent or guardian, provided organisations have other safeguards.

32. **Safeguards –** The Commissioner recognises the risk that children's data may be collected or shared without them being aware of this. She also has concerns that the online activity of children may remain visible to future employers or academic institutions. Robust safeguards are vital. The Commissioner believes organisations should provide assurance to the public, and where necessary to the ICO as the regulator, about how they manage data protection and privacy alongside innovation. Accountability is a new principle under the GDPR.

---

[3] Children's Commissioner report Growing Up Digital
https://www.childrenscommissioner.gov.uk/publication/growing-up-digital/

[4] HM Government's The Internet Safety Strategy – Green paper
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf

[5] https://ico.org.uk/media/about-the-ico/consultation-responses/2016/1625002/house-of-lords-children-and-the-internet-ico-response-20160901.pdf

33. **Privacy by design –** Privacy protections for children should be built into innovation by design and by default. Data controllers should think about children from the outset and take their potentially reduced capacity to assess the risks, benefits and consequences of the processing into account. Data controllers should take more responsibility for identifying and mitigating against the risks inherent in the processing, rather than expecting children to assess this all themselves.

34. **Data protection impact assessments –** Organisations processing significant amounts of personal data related to children should be regularly assessing the implications and effects of the processing on data subjects. The ICO has developed a Code of Practice for Privacy Impact Assessments. A requirement to conduct Data Protection Impact Assessments is part of the new GDPR.

35. **Transparency –** Transparency is a key consideration, reflecting the need for organisations to do more when aiming explanations at children and their parents. The Commissioner is also emphasising the importance of transparency of digital processing - including the use of big data, artificial intelligence and machine learning - where opaque or invisible practices can pose a particular risk to public trust and confidence.

36. ICO guidance emphasises the need to ensure that: children and their parents properly understand what personal data is being collected and how it will be used; any lack of understanding is not exploited; parental consent is sought when appropriate taking into account the risks of the processing; the collection of the personal data in question is necessary and not excessive; and default settings give a high level of privacy.

37. Social networking sites should explain their data collection practices in language that all users of their services are likely to understand and to invest in a high standard of security for all users. This should also include privacy settings by default (eg publication of data). Where it is clear that a service is aimed at children then the way the service is offered and the way it is explained must be age-appropriate. Services that are clearly aimed at children should not engage in data sharing with third part data brokers, no matter how simply the relevant choices are explained.

38. **Children's right to erasure –** There are no specific provisions within the Data Protection Bill about a child's right to erasure. Children will be able to exercise the right to erasure that is set out in Article 17 of the GDPR. Further details about the right to erasure within the GDPR are available in our Overview of the GDPR[6].

[6] ICO overview of GDPR https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-erasure/.

39. Where an organisation receives a request for erasure and it has disclosed that personal data to third parties, it must inform them about the erasure, unless it is impossible or involves disproportionate effort to do so. The GDPR reinforces the right to erasure by clarifying that organisations in the online environment that make personal data public should inform other organisations who process the personal data to erase links to, copies or replication of the personal data in question.

40. While this might be challenging, organisations that process personal information online, for example on social networks, forums or websites, must endeavour to comply with these requirements. To the extent that the data subject has provided data to separate data controllers themselves they would need to contact each controller separately to request erasure.

41. The ICO's existing experience with the right to erasure (or right to be forgotten) is in relation to requests for delisting of personal data from internet search results. Further detail can be found on our website[7]. This is likely to inform thinking and practically how complete erasure of personal data is under Article 17 of the GDPR. Erasure will only occur where the criteria in Article 17 are met.

42. In due course we will provide guidance to individuals about how to exercise their right to erasure. The process is likely to involve similar steps to those explained at the link above related to requests to search engines under the DPA 1998. As a matter of best practice we are also encouraging data controllers to develop tools such as dashboards to allow individuals to exercise their rights themselves online.

43. Recital 65 of the GDPR explains: 'that right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child'.

44. A child may exercise the above rights on their own behalf as long as they are competent to do so. Clause 187 of the Bill specifies that children in Scotland will be presumed to be competent unless the contrary is shown. This presumption does not apply in England, Wales or in Northern Ireland, where competence is assessed depending upon the level of understanding of the child, but it does indicate an approach that will be reasonable in many cases.

[7] ICO website section on internet search results https://ico.org.uk/for-the-public/online/internet-search-results/

45. An adult with parental responsibility may exercise rights on behalf of a child only when the child is not competent to do so, or when a competent child has authorised them to do so. This applies in all circumstances, including in an online context where the original consent for processing was given by the person with parental responsibility rather than the child.

46. In practice, where an adult with parental responsibility asks for a copy of their child's personal data or attempts to exercise one of the child's other rights on their behalf, organisations that are satisfied that the child is not competent, and that the person who has approached them holds parental responsibility for the child, may respond directly to the adult.

47. The Commissioner recognises that there can be situations in which an adult requests deletion of information from a child's records for reasons that are actually more relevant to their own interests rather than those of the child. In those circumstances the ICO would consider the 'best interests of the child' to whom the information relates. However, the child's own view of their best interests is something we may take into account in appropriate circumstances (depending upon the age, understanding and maturity of the particular child).