IN THE MATTER OF THE DATA PROTECTION AND DIGITAL INFORMATION BILL

OPINION

INTRODUCTION

1. I am asked to prepare an Opinion for **defend digital me** (DDM) in relation to the Data Protection and Digital Information Bill (the Bill). DDM have concerns about various aspects of the Bill and how they may impact on the protections enjoyed by individuals under the current legislation set out in the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR) and associated international obligations.

2. I am asked to focus on the aspects of the Bill which appear to impact most greatly on the rights of individuals, and which appear to reduce the accountability of data controllers and processors.

3. I conclude that the overall direction of travel of the Bill is to reduce protection for individuals, to make data controllers less accountable for the way they process personal data, and to increase their access to personal data.

4. A big risk in the way key issues are dealt with in the Bill, is that control of data is often dealt with as a *product* to be exploited and used by data controllers, when in fact a key aim of data protection legislation is about the protection of access to the personal data of *people*. This Bill shifts the power balance away from people and towards businesses and to government. Legislators should bear this key point in mind when considering the Bill.

SUMMARY OF MAIN POINTS OF OPINION

5. The following points of concern are raised in this Opinion:-

   (a) The proposed change to the definition of 'personal data' in the Bill has the potential to mean that some data currently defined as 'personal' will in future be excluded from protections in the DPA 2018 and UK GDPR.

   (b) In particular there is potential for the definition of 'personal data' to change depending on who is processing data, and the Bill removes the need for a data controller to have an ongoing duty to consider whether retained data has become 'personal data'.

   (c) A list of 'legitimate interests' (mostly concerning law and order, safeguarding and national security) has been elevated to a position where the fundamental rights of data subjects (including children) can effectively be ignored where the processing of personal data is concerned.

   (d) The Secretary of State can add to this list without the need for primary legislation, bypassing important Parliamentary controls.

   (e) Business friendly interests, such as direct marketing, are now listed, without provisos, as interests which may be seen as 'legitimate' giving succour to commercial organisations, but no added protection to the personal data of individuals.

   (f) Loosening of requirements on purpose limitation will assist commercial and non-commercial organisations involved in research and re-using personal data obtained from third parties, but will do nothing to increase protection for individual data subjects.

   (g) The powers of the Information Commissioner are diluted in a way which provides less protection to data subjects, but much more power to the government to restrict and interfere with the role of the Commissioner.

<u>THE CHANGE TO THE DEFINITION OF PERSONAL DATA</u>

6. It is clearly of great importance how personal data is defined, because any protections owed pursuant to DPA 2018 and the UK GDPR will only be applied to data which falls within that definition. If the definition is made more restrictive then data which is currently defined as personal data will be excluded from, protection.

7. The current definition of personal data is contained in s3 DPA which states as follows:-

> (2) *"Personal data"* means any information relating to an identified or identifiable living individual
>
> (3) *"Identifiable living individual"* means a living individual who can be identified, directly or indirectly, in particular by reference to—
>
> (a) an identifier such as a name, an identification number, location data or an online identifier, or
>
> (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

8. The Information Commissioner's Office provides guidance on what these provisions mean:-

    - An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals.
    - A name is perhaps the most common means of identifying someone. However whether any potential identifier actually identifies an individual depends on the context.
    - A combination of identifiers may be needed to identify an individual.
    - The UK GDPR provides a non-exhaustive list of identifiers, including:
        - name;
        - identification number;
        - location data; and
        - an online identifier.
    - 'Online identifiers' includes IP addresses and cookie identifiers which may be personal data.
    - Other factors can identify an individual.

9. Answering the question 'Can we identify an individual **directly** from the information we have?' the ICO states that:-

- If, by looking solely at the information you are processing you can distinguish an individual from other individuals, that individual will be identified (or identifiable).
- You don't have to know someone's name for them to be directly identifiable, a combination of other identifiers may be sufficient to identify the individual.
- If an individual is directly identifiable from the information, this may constitute personal data.

10. Answering the question, Can we identify an individual **indirectly** from the information we have (together with other available information)?, the ICO states that:-

- It is important to be aware that information you hold may indirectly identify an individual and therefore could constitute personal data.
- Even if you may need additional information to be able to identify someone, they may still be identifiable.
- That additional information may be information you already hold, or it may be information that you need to obtain from another source.
- In some circumstances there may be a slight hypothetical possibility that someone might be able to reconstruct the data in such a way that identifies the individual. However, this is not necessarily sufficient to make the individual identifiable in terms of UK GDPR. You must consider all the factors at stake.
- When considering whether individuals can be identified, you may have to assess the means that could be used by an interested and sufficiently determined person.
- You have a continuing obligation to consider whether the likelihood of identification has changed over time (for example as a result of technological developments).

11. The ICO issues much more detailed guidance to help identify what is personal data, but even from the above bullet points it can be seen that there is a fairly sophisticated system in place for data controllers to apply and data subjects to rely upon.

12. The Bill proposes to add to the definitions as follows. First, new subsections would be included in section 3 DPA 2018. Subsection 3(3A) (added by clause 1(1) of the Bill) would state that:-

> An individual is identifiable from information "directly" if the individual can be identified without the use of additional information.

13. Next, subsection 3(3B) (also introduced by clause 1(1)) would state that:-

> An individual is identifiable from information "indirectly" if the individual can be identified only with the use of additional information.

14. An immediate comment about these proposed new subsections is that they appear to add nothing to the way the current definition is interpreted by the ICO in its guidance or by the Courts when they have been asked to consider whether data is personal data.[1] However, they do provide statutory clarifications for the terms 'directly' and 'indirectly'.

15. Second, clause 1(2) of the Bill proposes to add a new s.3A to the DPA 2018 'for provision about when information relates to an identifiable living individual'.

16. New section 3A would limit when it can be said that information being processed is information 'relating to an identifiable living individual' to two circumstances.

17. Whether a living individual is 'identifiable' is to be judged by whether this would have been the case for a controller or processor 'by reasonable means at the time of processing'. This provides a limit both on the efforts that a controller/ processor must make to ascertain whether an individual is identifiable, **and** on the time at which the exercise is to take place.

18. New subsection 3A(5) would also define the content of 'reasonable means'. This would be whether an individual 'is identifiable by the person by any means that the person is reasonably likely to use'. New subsection 3A(6) says that factors to be taken into account in determining what comes within this description would include 'the time, effort and costs involved in identifying the individual by that means, and the technology and other resources available to the person'.

19. Two immediate concerns are raised by these provisions. The first is that whether a person is identifiable or not would become a function not of an objective test applicable to all data controllers, but would depend instead on a much more subjective consideration of the means that a particular data controller might have at their disposal and how they say these are used. Therefore, for a data subject,

---

[1] For a summary of recent case law see: *NHS Business Services Authority v IC and Spivack* [2021] UKUT 192 (AAC)

anxious to protect their data, whether data is personal data or not may now depend on which data controller has the information, and the resources available to that data controller. In essence, what is now described as 'personal' data could be rebranded as anonymous data simply because of the attributes of the controller in possession of that data.

20. The second concern is one of temporality. The Bill introduces the concept of whether an individual is identifiable 'at the time of processing'. If that is applied there is no ongoing duty on a data processor to assess whether over time while the data is retained, there may have been changes in circumstances which mean that data which was not personal data at the time of processing, has later obtained such properties. Data that was anonymous at the time it was initially processed may, over time, allow an individual to be identified but, under the Bill, will not become personal data. This might happen in circumstances where the data can be combined with additional information (not available at the time of processing) so that a person can then be identified or identifiable. This is to be contrasted with what is set out above and described by the ICO as a 'continuing obligation to consider whether the likelihood of identification has changed over time'.

21. The other prescribed case for whether information relates to an identifiable individual (and so is personal data) is set out in what would be a new subsection 3A(3). This relates to a situation where a data processor knows, or ought to know, that 'another person will, or is likely to, obtain the information as a result of the processing' and that person would be likely to be able to identify an individual as a result (presumably by combining information with information already in their possession).

22. As has been pointed out by a number of commentators, these extended definitions of what is included as 'personal data' can exclude data which, at present, has at least a legal prospect of being personal data. Thus, data controllers are likely to latch on to the fact that if it can be shown that the data they hold would not have been identified at the time of processing 'by reasonable means' as personal data, then it can be treated as not being personal data. That would appear to give room for unscrupulous data controllers to make claims about what would amount to 'unreasonable means' which would be difficult to disprove by a potential data subject. And there is now explicit encouragement for a data controller to turn a

blind-eye to changes in the nature of data retained, because it is only 'at the time of processing' when consideration needs to be given to the question of whether data is personal data or not.

23. In my view, these proposed changes to the definition of 'personal data' in the Bill are focused on the needs and convenience of data controllers, providing limits and provisos on what will be called personal data, while not providing any greater protections to individuals whose data will be in the possession of controllers.

24. Further, the proposed changes risk the UK being in breach of the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which notably did not include the provisos and caveats that the government now seeks to place on the definition of what is personal data.[2]

LEGITIMATE INTERESTS FOR PROCESSING PERSONAL DATA

25. Once personal data is identified, there are statutory restrictions on its use, and it can be processed only in limited circumstances. It is worthwhile explaining what is currently contained in Article 6(1) of the UK GDPR, which sets out situations in which it is lawful to process personal data, as the Bill introduces significant changes to these.

26. As the ICO states: 'The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever you process personal data'. The ICO summarises the current bases in Article 6(1) as follows:-

    (a) **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose.

[2] See further https://amberhawk.typepad.com/amberhawk/2023/04/index.html

> (b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
> (c) **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).
> (d) **Vital interests**: the processing is necessary to protect someone's life.
> (e) **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
> (f) **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to
> perform your official tasks.)

27. It can be seen that Article 6(1)(f) has a wide potential for justifying processing of personal data. The actual wording of Article 6(1)(f) sets out a balancing test which permits processing for any 'legitimate interest' purpose, provided that the processing:-

> …is necessary for those interests, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

28. In effect, for the purposes of Article 6(1)(f), a person's personal data is protected from processing unless:-

    (a) There is a legitimate interest in processing the information.

    (b) Processing is 'necessary' for that interest (ie the interest cannot be achieved by any other means).

    (c) Those interests override the fundamental rights and freedoms of a person (which will include rights to privacy and an expectation that personal information will not be disclosed). Note also the particular emphasis placed on the rights of a child who is a data subject.

29. Clause 5 of the Bill inserts a new criterion for lawful processing of personal data just before Article 6(1)(f), and entitles it Article 6(1)(ea). It states that processing is lawful where:-

> (ea) processing is necessary for the purposes of a recognised legitimate interest.

30. Thus, so long as the legitimate interest is 'recognised' and processing is 'necessary' for that legitimate interest, there will be no requirement to carry out the balancing test with the data subjects 'fundamental rights' before processing of the personal data is lawful. That includes a situation where the data subject is a child.

31. Given this formulation, it is important to know which legitimate interests are, in fact, 'recognised'. The Bill provides for this by adding a new sub-Article to the UK GDPR: Article 6(5), which states that processing is necessary for the purposes of a recognised legitimate interest only if it meets a condition which is set out in a new Annex to the UK GDPR.

32. As currently drafted these recognised legitimate interests include processing necessary for national security, public security and defence; detection, investigation and prevention of crime; responding to an emergency; safeguarding vulnerable individuals and for democratic engagement. To be clear, if the Bill is passed into law these legitimate interests will not require incorporation of the 'balancing test' that features in Article 6(1)(f) UK GDPR, and which gives particular emphasis to the fundamental rights of children.

33. I note that no justification has been provided for lifting these specific interests into a special category where fundamental rights of individuals are not relevant. Although it might be considered that the current listed interests (focusing as they do on law and order, national security and safeguarding) might often include factors which would outweigh individual rights, there is no guarantee that this will always be the case, and the Bill's proposals would appear to constitute an unwarranted side-stepping of fundamental rights in circumstances where, they will often be especially relevant.

34. Article 6 of the UK GDPR is also to be amended to allow the Secretary of State to add to this list of legitimate interests which do not require the 'balancing test'. This would not require primary legislation – the Secretary of State would be able to add to the list by secondary legislation, subject only to the affirmative resolution procedure in Parliament. Although the Secretary of State will have to have 'regard to' fundamental rights of data subjects and the rights of children in particular before adding to the list, this still provides a wide discretion, with the potential for fundamental rights to be put at risk in a growing number of areas, without proper democratic scrutiny. This is an area which clearly alarms the European Commissioner which says it is a matter 'which raises questions with respect to the level of protection' and that concerns have been raised with the UK Government. [3]

35. In relation to 'legitimate interests' which will still be covered by Article 6(1)(f), there remains a question as to whether any particular interest is 'legitimate' so as to justify the potential processing of personal data (subject to the requirement of 'necessity' and the fundamental rights 'balancing' test). The Bill (clause 5(4)) seeks to amend Article 6 GDPR by providing for a new paragraph 9 to the Article which lists 'examples of types of processing that may be processing that is necessary for the purposes of a legitimate interest'.

36. The non-exhaustive list of scenarios where organisations may rely on the legitimate interests lawful basis, includes for the purposes of (a) direct marketing; (b) transferring data within the organisation for administrative purposes (inter-group transmission of client or employee information); and (c) ensuring the security of network and information systems. It is important to note that the necessity and balancing tests will still need to be met. Inter-group transmission can include processing in as wide a context as 'between members of a group of institutions affiliated to a central body.'

[3] EN E-001790/2023, Answer given by Mr Reynders on behalf of the European Commission (2.8.2023)

37. These specific references give succour to the business community where it is has not been entirely clear which interests might be considered as 'legitimate' (although direct marketing was included in the recitals to the GDPR as an example (see recital 47)). The specific reference to these matters in primary legislation will give added confidence to those involved in direct marketing that their purpose will be seen as a legitimate interest. Once again comfort is given to the data controller (often in the business sector), and an increased risk passed to individuals that their personal data will be processed without their consent.

38. The list in new Article 6(9) is not exclusive and the Explanatory Notes to the Bill also confirm that data controllers may rely on Article 6(1)(f) to process personal data for other legitimate activities, if the processing is necessary and the balancing test is carried out (without, of course, defining what else is included in the definition of 'legitimate').

39. These additional provisions do not set in stone that the interests listed will be seen as 'legitimate' if challenged. However, the government's decision to include matters such as direct marketing in the Bill itself is a strong indication as to what it is thought should be considered as legitimate. This approach is another example of the Bill favouring and supporting those who might be involved in the processing of large amounts of personal data, while providing nothing to shore up the protections offered to individual data subjects. Concerns about the lack of understanding about the assessment and application of the legitimate interest test have been expressed by the ICO in past reports, including in relation to government departments (see the February 2020 data protection audit report in relation to the Department of Education, for example[4]).

[4] https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618384/department-for-education-audit-executive-summary-v1_0.pdf

40. It is also important to remember in debates about the Bill that Art 6 does not contain the only restrictions on data sharing that may be relevant to a public body, for example. If there are other statutory restrictions on a public body processing information, these will act as further bars on that body, even if the provisions in Article 6 are fulfilled. In my view this should be made clear in the Bill, to prevent the mistaken belief that Article 6 provides the only relevant statutory framework for the purposes of data processing.

PURPOSE LIMITATION (IN RELATION TO FURTHER PROCESSING)

41. One of the key principles contained in Article 5 of the UK GDPR is a concept known as 'purpose limitation' so that when personal data is collected for one purpose, there are restrictions on what it can be used for thereafter.

42. Thus, as currently drafted, Article 5(1)(b) states that personal data shall be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes' subject to a proviso that 'further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall…not be considered to be incompatible with the initial purposes'.

43. Clause 6 of the Bill amends Article 5(1)(b) so that it would read that personal data shall be:-

> collected (**whether from the data subject or otherwise**) for specified, explicit and legitimate purposes and not further processed **by or on behalf of a controller** in a manner that is incompatible with **the purposes for which the controller collected the data**' (changes emphasised).

44. The effect of this wording is that a data controller will now only have to consider the purposes for which it collected the data. If the controller obtained the data from another controller, it will not need to consider the purposes for which that

other controller may have originally collected the data. Thus, for example, if an organisation is researching information obtained and contained on a public register for its own purposes, it will not have to consider the reasons why the information was obtained in the first place.

45. This is a significant change and lessens the protections under which personal data is held. Data protection standards for decades have required subsequent use to be 'not incompatible' with the original purpose for collection. For example, the OECD 1980 Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data state that:

> **Purpose Specification Principle**
>
> 9.The purposes for which personal data are collected should be specified not later **than at the time of data collection and the subsequent use limited to the fulfilment of those purposes** or such others as are **not incompatible with those purposes and as are specified on each occasion of change of purpose**.[5] **(emphasis added).**

46. However, the new Bill creates a new set of conditions under which the processing of personal data for a new purpose is to be treated as processing in a manner compatible with the original purpose. Clause 6 of the Bill sets out the conditions for determining whether the reuse of personal data (otherwise known as 'further processing') is permitted in compliance with the purpose limitation principle outlined in Article 5(1)(b) of the UK GDPR. The conditions are made by way of a series of amendments to the UK GDPR.

47. Key to the amendments is a proposed new Article 8A to the UK GDPR (introduced by clause 6(5) of the Bill) for the purposes of setting out the conditions under which further processing of personal data complies with the purpose limitation principle in Article 5(1)(b). The Bill (through this new Article) would add a new Annex to the UK GDPR listing situations in which processing is to be treated as compatible with

[5] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

the original purpose. In summary, those situations would be where processing is necessary:-

(a) to make a disclosure of data to a public authority requesting the data in reliance upon the 'public task basis';
(b) to protecting public security, or responding to an emergency;
(c) to protect the vital interests of the data subject or another individual;
(d) to safeguard a vulnerable individual; for the purposes of assessing or collecting tax; and
(e) for the purposes of complying with the controller's legal obligations.

48. In addition to the list in that Annex, the Bill also provides that a new purpose is compatible with the original one if the new purpose is to safeguard one of a number of public interests listed in Article 23(1)(c) to (j) to UK GDPR (largely to do with law enforcement and national security) and the processing is authorised by law.

49. As seen above, processing for the purposes of scientific or historical research or archiving in the public interest or for statistical purposes will be compatible with the original purpose of the processing. However, 'scientific research' and 'scientific research purposes' would now be defined by clause 2 of the Bill to mean 'any research that can reasonably be described a scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity'.

50. Although the Bill restates requirements for researchers to put in place certain safeguards for the rights of data subjects whose data is used in research, the Bill provides scope for researchers to seek more open-ended consent from data subjects to use data for a particular area of scientific research without having to be able to fully identify the purposes of the research.

51. Once again the Secretary of State will have the power under new Article 8A(5) to amend the list of conditions in the Annex that are to be treated as compatible with the original purpose. The power enables the Secretary to add to or vary the conditions or omit conditions added by regulations without full scrutiny by Parliament.

52. The provisions in relation to purpose limitation and the wide clarification of what is defined as research, continues the themes in other parts of the Bill. Processors will find that (a) they only have to consider the purpose for which they collected the data when considering new purposes; (b) that some purposes will be automatically compatible with the original purpose for which data was collected; and (c) researchers especially may find it easier to establish that their purposes are automatically compatible. The explicit acknowledgment that automatically compatible scientific research can be for commercial purposes as well as non-commercial purposes will be welcomed by the research industry which will see benefits in the loosening of barriers around sharing scientific research data.

53. However, it is clear that these 'clarifications' in the Bill benefit data processors and controllers while providing no new protections for individual data subjects. In situations, especially where purposes will become automatically compatible, data subjects will lose important rights currently in play, such as the rights to be informed, to rectify, to restrict and to object to data processing.

<u>THE ROLE OF THE COMMISSIONER</u>

54. The Commissioner plays a key role in the oversight of the government's handling of data so it is vital that the role is completely independent from government. However, clause 27 of the Bill (amending the 2018 Act) dilutes the Commissioner's freedom to protect the rights of data subjects.

55. First of all, in carrying out the functions under the data protection legislation the Commissioner would have to have regard to a range of matters. These are as follows:-

(a) the desirability of promoting innovation;
(b) the desirability of promoting competition;
(c) the importance of the prevention, investigation, detection and prosecution of criminal offences;
(d) the need to safeguard public security and national security.

56. Although the principal objective of the Commissioner is set out to be (a) to secure an appropriate level of protection for personal data, having regard to the interests of data subjects, controllers and others and matters of general public interest, and (b) to promote public trust and confidence in the processing of personal data, it can be seen that the rights of data subjects are given no particular primacy in this formulation and could get lost amongst the range of other issues and interests that must be taken into account.

57. Secondly, clause 28 will give the Secretary of State new powers to issue instructions to the Commissioner and to interfere with how it functions. For instance, the government will be given the power to issue a statement of strategic priorities to the Commissioner. There is no guidance in the Bill as to what those strategic priorities can cover, but whatever they are, the Commissioner must have regard to them when carrying out functions, and the Bill requires the Commissioner to respond in writing as to how they will be addressed. it will address them.

58. Additionally, the Commissioner will have to seek the approval of the UK Government (rather than simply consulting) before issuing Codes of Practice: see clause 29 of the Bill.

59. All of this constitutes a significant interference with the independence of the Commissioner. Where the government of the day and the secretary of state are champions of data protection and data subjects' rights, then clearly these powers can be used to guide the Commissioner to be an effective regulator. But equally they provide a platform and a framework for a government seeking to undermine data protection rights to effectively hamstring a Commissioner by issuing strategic priorities which make the Commissioner's task more difficult, or which concentrate on the rights of controllers, and by refusing to agree to Codes of Practices which do not reflect the government's restrictive views on data protection rights. It is not surprising that the EU Commission commented on 2 August 2023, that this is one of the areas which will 'raise questions with respect to the level of protection' provided to data subjects and about which the Commission has 'repeatedly' raised concerns with the UK government and that the changes 'affect the independence' of the Commissioner.[6] To date the government has not been prepared to recognise these

---

[6] See footnote 3.

concerns, and legislators will want to closely scrutinise what amounts to a power-grab by the government of the Commissioner's functions.

SPECIFIC CONCERNS ABOUT CHILDREN'S DATA

60. What is described in this advice is a new legislative framework which has the capacity, often through secondary legislation, to loosen the protections on personal data and its use. I am instructed that DDM has a particular interest in the protection of the personal data of children, and over the years has sought particular measures to enable this protection.

61. If the new definition of personal data (as described above) is enacted that will also, of course, mean that fewer data of children will be protected under the new law.

62. It has already been seen in this advice that protections on the use of personal data have been loosened by clause 5 which introduces the category of a 'recognised legitimate interest' for processing where a 'balancing test' (as required under the current law, and giving particular emphasis to the fundamental rights of children) is no longer required. With new initiatives linked, for example, to the use of artificial intelligence (AI) 'to help schools to understand their pupils better and analyse the impact of innovations', there is a need to be clear about the principles that should be followed,[7] and not the time to be relegating children's rights to be protected only at the discretion of the government (see paragraph 34 above),

63. There are other particular concerns in relation to children, such as powers under the Bill (clause 87) which would enable the Secretary of State to make regulations for registered political campaign groups, of any kind, to send unsolicited digital, email, and print direct marketing to teenagers (age 14+) across all of the UK.

64. Recognising the special position of children, and the vulnerability of their data, DDM in its briefing for the second reading of the Bill and before the House of Lords, has produced a number of case studies where there is concern about the processing of children's data in particular in educational and social care contexts. DDM has identified a number of occasions where the Department of Education

[7] https://schoolsweek.co.uk/minister-wants-schools-to-benefit-from-ai-revolution/

does not carry out Data Protection Impact Assessments (DPIA) in circumstances where this should happen. There are concerns that the DfE misuses national pupil records, outside the uses for which it is empowered to hold the records, for the purposes of immigration enforcement.[8]

65. As a result, DDM has advocated for a Code of Practice on pupil data on a number of occasions when legislation about data protection has been before Parliament. For example, when the Data Protection Act 2018 was being dated an amendment was proposed to introduce a Code on processing personal data in education where it concerns a child or pupil which provided as follows:-

> The Commissioner must consult on, prepare and publish a code of practice on standards to be followed in relation to the collection, processing, publication and other dissemination of personal data concerning children and pupils in connection with the provision of education services in England, within the meaning of the Education Act 1996, which relates to the rights of data subjects, appropriate to their capacity and stage of education.

66. The best way to protect children's data is by the retention or introduction of specific safeguards in legislation. However, there is no doubt in my mind that, additionally, such a code of practice as previously advocated for by DDM would be a useful tool for ensuring that special care is taken when the processing of the personal data of children within the education and social care systems (especially) is under consideration.

CONCLUSION

67. Protection of personal data is a fundamental individual right, which increasingly needs to be safeguarded in a world where the processing of mass and bulk data by organisations and public bodies is becoming the norm. Protection of personal data is covered not only by the data protection provisions, but also by the right to respect for private life enshrined in Article 8 of the European Convention of Human Rights (as

---

[8] https://defenddigitalme.org/2023/03/21/call-for-action-from-the-uk-information-commissioner-to-uphold-childrens-rights-in-the-hostile-environment/

part of UK law by virtue of the Human Rights Act 1998), and common law rights such as the tort of misuse of private information.

68. In my view, the proposals of this Bill are not designed to enhance these individual rights as might be expected, but appear to be designed to loosen the safeguards on the use of personal data for big business and government. These data protection reforms will make our personal data more available for commercial benefit, while putting our personal privacy at risk. They provide government with the power to add to the reforms without the need for further primary legislation, and likewise to control the ambit and work of the Information Commissioner. The Bill could make it more difficult to exercise data protection rights, establish that information is personal data, contest an automated decision, or seek administrative redress in the UK, while giving the government of the day the power to loosen protections even further without proper parliamentary scrutiny.

69. Overall the Bill is a significant shift away from a rights-based regime towards a set of market standards which treats data a product, raising concerns that the UK is moving away from international benchmarks and standards.

70. In my view there must be very careful scrutiny of the proposals in the Bill to ensure that fundamental rights are not eroded, and proper restrictions and limitations remain placed on those who seek to access, retain and use our personal data.

STEPHEN CRAGG KC

Doughty Street Chambers

22 November 2023