Written Evidence by the National Data Guardian (DPDI0008)

Introduction

This is the National Data Guardian's (NDG's) formal response to the House of Commons Public Bill Committee's call for written evidence in relation to the Data Protection and Digital Information (No.2), which is currently passing through Parliament.

This is not an exhaustive review of all clauses within the Bill, but rather the NDG's considerations on
those areas of the Bill that may impact the health and social care sector.

As the Bill follows the Department for Digital, Culture, Media and Sport's (DDCMS) 2021 consultation, 'Data: a new direction' on the proposed reforms to data protection law in the UK, we wish to refer the Committee to the NDG's response submitted to DDCMS on 19 November 2021.

The European Commission's decision on the adequate protection of personal data by the United Kingdom notes that 'provisions providing the rights of the individuals have been maintained in the UK GDPR without material changes'.[1] Maintaining adequacy is essential if the government is to achieve their stated aims. Any significant departure from existing rights provided for by UK GDPR could trigger a review of the existing EC decision, creating uncertainty for health and social care organisations, particularly in the area of research.

[1] European Commission, Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom.

1 Personal data and Article 8 of the European Convention on Human Rights

1.1 The Bill would make changes to the rights of data subjects under the UK GDPR, including altering the threshold at which data controllers may refuse to comply with a request made by a data subject and expanding when personal data can be processed for a reason other than that for which it was originally collected. Would these changes have any implications for data subjects' right to respect for their private lives under Article 8 ECHR?

Altering the threshold at which data controllers may refuse to comply with a request made by a data subject.

The existing threshold for refusing a request made by a data subject is that a request must be manifestly unfounded or excessive. The Information Commissioner's Office (ICO) states that requests from data subjects may be manifestly unfounded where there is no intention to exercise one's right of access or has no other purpose than to cause disruption. Manifestly excessive means that a request must be clearly or obviously unreasonable considering the circumstances of the request.[2]

Reconsidering the threshold for refusing a request from a data subject may be helpful to many organisations. However, it is important to strike a balance between individual rights and organisational obligations.

The Bill would create a list of considerations for refusing a data subject request by virtue of new Art 12A, 'Vexatious or excessive requests'. It is questionable, based on Art 12A(4), whether vexatious applies the same threshold for refusal as manifestly unfounded or excessive.

It could be argued that including criteria such as 'the resources available to the controller' or 'the relationship between the data subject and the data controller' does not create an objective test under which the legislation can ensure data subject rights are complied with consistently.

Vexatiousness has been thoroughly considered under Freedom of Information law. It is generally accepted that the starting point is whether a request has a reasonable foundation. It requires an assessment of each individual case. Even in the event of an improperly motivated requester, if the information is considered so important and aligned to what the legislation is designed to achieve, disclosure is required.[3] The vexatious or excessive requests assessment criteria under Art 12A do not

[2] Information Commissioner's Office, When can we refuse to comply with a request <https://ico.org.uk/for- organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/when-can-we-refuse-to- comply-with-a-request/> Accessed 25 May 2023.

[3] Dransfield v The Information Commissioner, Devon County Council [2015] EWCA Civ 454, [68].

consider the extent to which the information would be of value to the requester or acknowledge the importance of these fundamental rights under data protection law.

The ability for data controllers to consider charging a fee for vexatious requests is also worrying. The NDG previously outlined her position on fees in detail when providing a response to the DDCMS consultation in November 2021. This position still stands. Introducing fees has the potential to be unfair and discriminatory. Any fee regime could be inherently prohibitive, especially for those with limited financial means. There may also be unintended consequences in respect of data subjects having the ability to exercise other data protection rights. For example, an individual's right to have their data rectified is only possible if an individual knows what data is held about them.

Careful consideration must be given to the design of such measures to ensure they only limit rights in exceptional circumstances that represent an unjustifiable burden on organisations. Any departure from existing thresholds for limiting an individual's rights could influence the EU's adequacy decision, creating uncertainty for health and care organisations and an additional burden of having to consider the thresholds of two separate regulatory frameworks.

Expanding when personal data can be processed for a reason other than that for which it was originally collected.

Clause 5 of the Bill amends UK GDPR Article 6(1)(e) to make clear that a task in the public interest must be that of the data controller.

Schedule 2 of the Bill would introduce Annex 2 into UK GDPR, the purpose of which is to outline when processing is to be treated as compatible with the original purpose.

Paragraph 1 of Annex 2 would make disclosures of personal data, following a request from another data controller, compatible on the basis that the requesting data controller requires that information for a task in the public interest or in the exercise of official authority.

It is not immediately clear when or how the government envisage this provision will be utilised, or what the intended benefits are. However, we are concerned that by making disclosures compatible when aligned to the requesting data controller's public tasks, irrespective of the purpose at the point of data collection, the threshold for sharing by public authorities will be somewhat diminished.

Although disclosures would still be subject to some limited criteria as provided for in Annex 2 para 1(b), the assessment becomes focused on the needs of the requesting controller, as opposed to the respect for the rights of the individual.

Whether further processing is deemed compatible with its original purposes usually requires an assessment under UK GDPR Art 6(4). This assessment requires (amongst other things) a data controller to consider: the possible consequences of the intended further processing for data subjects; the relationship between the data controller and the data subject; and the existence of appropriate safeguards such as pseudonymisation.

Trust is an integral element of an effective health and care system. Patients and service users must be able to disclose the most intimate details about their lives to enable safe care and effective treatment. If there is any indication that their health and care data may be disclosed for reasons

other than their care without due regard and subject to sufficient safeguards, this could have severe consequences for the effectiveness of the health and social care system.

1.2 The Bill would create a new lawful ground for processing personal data, where it is necessary for a "recognised legitimate interest". Processing on this ground would not be qualified by the overriding interests or fundamental rights of the data subject. Does this proposed change in the law raise any concerns about compatibility with human rights, including under Article 8 ECHR?

Legitimate interests is one in a series of lawful bases available that can be relied upon for the general processing of personal data. The NDG is supportive of initiatives that encourage the safe and appropriate sharing of health information, provided the rights of individuals are not diminished.

In the case of South Lanarkshire Council v The Scottish Information Commissioner, Lady Hale considered 'the proper interpretation' of legitimate interests. She suggested that three questions must be answered, namely:

(i) 'Is the data controller, or the third party or parties to whom the data are disclosed pursuing a legitimate interest or interests?
(ii) Is the processing necessary for those purposes?
(iii) Is the processing unwarranted in this case by reason of prejudice to the rights and freedoms or the legitimate interests of the data subject.'[4]

The test is, therefore, one of reasonable necessity, applying the least restrictive means to achieve a legitimate aim.[5] Removing any consideration of balance here could be problematic. We feel that dilution of the requirements of Recital 47 UK GDPR, which include the need for a 'careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that the processing for that purpose may take place' could significantly diminish the protection of personal data.

The approach to legitimate interests assessments (LIA) outlined by the ICO demonstrate the importance of balancing the legitimate interests of organisations in personal data with the fundamental rights of the data subject. The removal of the need to make a LIA could have significant implications for the protection of personal data. Without the requirement for data controllers to ensure they have valid justifications that not only require them to evidence a valid purpose, but also

[4] South Lanarkshire Council v The Scottish Information Commissioner [2013], UKSC 55 1 W.L.R. 2421, [18].

[5] Goldsmith International Business School v Information Commissioner and the Home Office [2014] UKUT 563 (AAC) [35-42].

to justify the type and volume of data that is processed, the rights of the individual could be limited in a significant way by the Bill.

It is not clear to what extent processing based on a recognised legitimate interest as per Schedule 1 of the Bill will limit one's right to object to processing. As per UK GDPR Art 21(1), a data subject shall have the right, on grounds relating to his or her personal situation, at any time to object to the processing of personal data concerning him or her which is based on point (e) or (f) of Art 6(1).

The NDG recognises that the right to object is not absolute.[6] However, where an objection is raised, data controllers can only continue to process personal data subject to an objection where they can demonstrate 'compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject'.[7]

2 Other concerns

2.1 Research - Transparency requirements for further uses of data for research

The government's 2021 consultation considered replicating GDPR Art 14(5)(b) in Article 13. Currently, Article 14(5)(b) has the effect of relaxing requirements regarding the provision of transparency information where personal data have not been obtained from the data subject to the extent that it would be impossible or would require disproportionate effort.

The Bill would relax requirements regarding the provision of transparency information where personal data are collected directly from the data subject, and those data are subsequently processed for Research, Archiving and Statistical purposes.

Disapplying transparency requirements could be argued to be at odds with the requirement under Art 5(1)(a) to ensure processing of personal data remains lawful and transparent. As such, we would urge the government to consider the compatibility of this provision with the broader obligation within UK GDPR.

There should be a high bar on what is considered disproportionate effort where personal data has been collected from the data subject. This is because collecting personal data from a data subject will usually provide opportunities to communicate transparency information to them. It is not clear that new provisions incorporated by Clause 9 of the Bill set this bar sufficiently high. For example, the number of data subjects does not inherently make communication more difficult, and the use of

appropriate safeguards does not equate to fairness if the processing is not aligned to what an individual might reasonably expect, especially where there is a reduction in transparency.

The government should be mindful of the correlation between trust and transparency. At a time when a lack of transparency has caused important projects that use health data for public benefits to fail or stall due to a breakdown of public trust, this is especially important.

Where data is repurposed for research, it is important that existing protections for personal data reused for research are not diminished; this could have a detrimental impact on the public's trust in those organisations that might make data available for research purposes.

2.2 Research – broad consent for research

Consent is not ordinarily relied upon as the legal basis for processing personal data for health research purposes. As such, this new definition provided for in Clause 3 of the Bill may cause some confusion about the relationship with existing lawful bases that are relied upon for health research, and the additional safeguards they afford.

Relying on the research provisions of Article 9 to undertake scientific research encompasses significant safeguards. Any dilution of this in favour of a broad concept of consent could diminish the safeguards and transparency requirements for processing data for research purposes.

30/05/2023