Department for Science, Innovation & Technology

Viscount Camrose
Parliamentary Under Secretary of State
Department for Science, Innovation & Technology
100 Parliament Street
London SW1A 2BQ

www.gov.uk/dsit

11th April 2024

House of Lords
London
SW1A 0PW

My Lords,

Thank you for your continued engagement with the Data Protection and Digital Information (DPDI) Bill during the first three days of Committee stage. I am writing to follow up on questions raised by Noble Lords during the debate, to which I have provided a more detailed response below. I am copying this letter to all noble Lords who were present during the first three days of Committee stage and will deposit a copy in the House Library.

The Government's policy on data communities

I will first address Lord Clement-Jones' request to provide more detail on the government's policy on data communities.

I recognise that data communities, as part of the broader data intermediaries sector the Government is already engaging with, have the potential to empower individuals to exercise their data subject rights. In addition to data communities, intermediaries include data cooperatives, data exchanges, data trusts, and trusted third parties. Furthermore, existing data protection law does not prevent collective exercise of data rights such as the right to portability, the right of access, and the right of erasure, nor the delegation of these rights.

Therefore, the Government does not want to limit the rapidly developing data intermediaries sector by adopting a definition of data community aside from any other type of data intermediary, or by requiring the ICO to establish a code of practice and introduce a registration and complaints process before sufficient consultation with the

ICO, data intermediaries, data controllers and individuals has taken place, as this may result in unnecessary burdens on a developing business model.

I want to assure you that the Government is committed to continue working with different types of intermediaries, including data communities, as well as academics, regulators, civil society and the private sector to establish if the sector indeed requires a more specific regulatory framework to enable its development and protect individual data rights.

Clarifying reforms to the definition of personal data

Second, I will answer Lord Bassam's concerns about whether the Government had conducted an assessment of the impact of reforms in clause 1.

The Government's impact assessment for the Bill includes the measures in clause 1, and refers to them as adopting the test from existing Recital 26 to the GDPR into legislation, which states: *"To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."*

ICO guidance on identifiability largely repeats this formulation. This relative position, where identifiability is informed by the reasonable means likely to be used by the controller or processor, is one that the Government has replicated on the face of the legislation in clause 1. To be clear, neither the current position nor the drafting of clause 1, allows for the subjective intention of the controller or processor to determine whether data is identifiable.

Equally, the definition of "processing" in the data protection legislation is very broad, and includes collection, alteration, retrieval, storage, and sharing. Therefore, the reference in clause 1 to "the time of processing" clarifies that determining identifiability is a continuous activity with ongoing obligations for controllers and processors.

This means that data cannot be considered anonymous if at any point during its processing cycle, such data can be re-identified by reasonable means by either the controller or processor, or by someone likely to obtain the data. This again replicates the language in Recital 26, under which there is also an ongoing obligation on

controllers and processors to consider whether they hold personal data.

The aim of clause 1 is to increase confidence for organisations that anonymise data, by placing the existing test, which is consistent with ICO guidance, caselaw and recitals to the GDPR, on a legislative footing.

Savings from reforms to Subject Access Requests

During the committee hearing, I stated that the savings from the reforms to the wording of SARs are valued at "less than 1% of the benefit of more than £10 billion that the Bill will bring".

The March 2023 impact assessment estimates the cost savings from limiting the time and threshold for responding to subject access requests to be between £9.3 million and £153.0 million per year, with a medium estimate of £59.1 million per year. The £59.1m figure is indeed less than 1% of the 10-year Net Present Value (NPV) of the DPDI Bill, which is over £10 billion.

However, I have since been advised that a more accurate approach when comparing the value of these reforms to the total benefit of the Bill is to use 10-year discounted compliance cost savings, rather than the annual cost savings. Using this method, the savings from the reforms to the wording of SARs are valued at less than 4% of the 10-year NPV rather than less than 1%.

Government minor and technical amendments

I will now turn to the questions raised by Lord Bassam about the minor and technical amendments to the Bill.

a. **Definition of 'Further Processing'**

In connection with amendment 20, Lord Bassam queried the meaning of "further processing" and whether it has the same meaning as the reuse of personal data. He also queried whether the Bill would restrict further processing for purposes not in line with the original purpose for which the data was collected and the extent to which data subjects are informed of this processing. I can confirm that further processing is the technical term for personal data collected for one purpose and reused for a different purpose, and that the purpose limitation principle will continue to apply to the processing of personal data, subject to the rules and exceptions set out in Clause 6

of, and Schedule 2 to, the Bill. The transparency principle will also continue to apply including the requirement of data subjects to be informed about further processing as set out in Article 13 and 14 of the UK GDPR.

b. Scope of Regulation-Making Powers for Smart Data

Lord Bassam asked for clarity on whether Amendment 196, which affects Clause 96(3), would further extend the Secretary of State's power to make regulations to impose levies in relation to Smart Data. I can assure the Committee that amendment 196 does not extend the power to impose the levy any further. The amendment extends the existing safeguard in clause 96(3) to cover authorised persons and third party recipients. This is necessary in light of the previous extension of clause 96(1) to cover those groups.

c. Clarity on Interpretation of Time Periods

The Government's amendments make clear that the EU-derived rules on the interpretation of time periods set out in the Time Periods Regulation continue to apply to the UK GDPR and other regulations that form part of the UK's data protection and privacy framework. Lord Bassam asked for more information on the purpose of these amendments. He also queried why Amendment 253 applied domestic rules on time period interpretation in certain situations.

The approach in the Time Periods Regulations is not appropriate for calculating some timings – for example, the meaning of financial year. Amendment 253 therefore applies the domestic approach.

d. Limits on the Information Commission's powers

The Government also introduced an amendment which confers a general incidental power on the Information Commission to do anything it considers appropriate for the purposes of, or in connection with the exercise of its functions. Lord Bassam asked for more information on the limits and scope of this power.

Where specific powers have been expressly conferred on a statutory corporation (as it is the case with the Information Commission), it is now standard practice to make express provision in relation to incidental powers to avoid an inference that the list of specific powers is intended to be exhaustive.

Without an explicit power, the Information Commission would still have the implied power to do things incidental to the exercise of its functions, for example hold land and other property and enter into agreements. This amendment merely makes those implicit powers explicit for the avoidance of doubt. It does not give the Information Commission substantive new powers.

Protections for Children's Data

Baroness Kidron asked for an explanation on how clause 5 applies to and maintains appropriate protections for children's data when used for direct marketing purposes.

Subsections 9 and 10 of clause 5 deal with direct marketing. They simply provide a list of examples of common commercial processing activities that "may" constitute legitimate interests, and this list includes direct marketing. These examples are drawn directly from the existing recitals to the GDPR, and do not make substantive changes to the current legal position.

So, while the Bill clarifies that direct marketing may constitute a legitimate interest, organisations must still carry out the legitimate interests balancing test to ensure that the legitimate interests ground can be relied on for the processing before it begins. The age of the recipients of the marketing, whether they would expect to receive the marketing, and the potential impact it could have on them will all be pertinent factors in this assessment.

ICO role in Protecting Children

Baroness Kidron asked me to explain in what ways the ICO can use its old instruction to uphold the current safety for children.

Firstly, through Article 57(1)(b) it remains a statutory requirement on the ICO to promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing for all persons. This requirement states directly that activities addressed specifically to children shall receive specific attention. In line with this statutory task, the ICO recently set out priorities to protect children's privacy online, highlighting that safeguarding children's personal data is a key priority.

Secondly, under Section 126(D) of the Data Protection Act 2018, the Commissioner is required to keep under review each code that is issued under section 125(4)

including the Age-Appropriate Design Code whilst it is in force. The Information Commissioner's Office may keep the AADC up to date in response to emerging technologies — including Artificial Intelligence — and to reflect any legislative changes. As part of the implementation of the DPDI Bill, the Commissioner is required to update his guidance to ensure that they comply with the new provisions introduced by the Bill.

The Information Commissioner is held to account overall by the Parliamentary Select Committees, before which the Commissioner usually appears two to four times per year.

Secretary of State powers in relation to Automated Decision Making

Lord Clement-Jones asked me to explain the rationale for providing the Secretary of State with powers to regulate Automated Decision Making (ADM). The Government has provided the Delegated Powers and Regulatory Reform Committee with detailed memoranda setting out the context and purpose of each power in the DPDI Bill, and the Government's justification for it. The powers related to automated decision making are at paragraphs 47 – 75. In general, Noble Lords will be aware that data protection law is principles based and, when considering the fast-moving advances and adoption of technologies relevant to ADM in particular, it is important the law is able to adapt as technology advances.

The Government has noted the report on the Bill by the Delegated Powers and Regulatory Reform Committee, which discusses the Secretary of State power to vary the safeguards in Article 22D. May I reassure noble Lords that I will address this in more detail in my response to the Committee's report, which will be published shortly.

Public sector compliance with Algorithmic Transparency Recording Standard

Lord Clement-Jones asked what compliance and accountability mechanisms will be put in place to ensure that government departments abide by the Algorithmic Transparency Recording Standard (ATRS). It focuses on algorithmic tools which influence decision-making processes with direct or indirect public effect, or which directly interact with the general public.

Government bodies are increasingly using algorithmic tools to support and optimise their decision-making processes. However, providing accessible information on the use of these technologies in a trusted and effective way is often difficult. The ATRS. addresses this gap by enabling public bodies to publish details about the algorithmic tools they use proactively and to make this information accessible to everyone. It is one of the world's first interventions for transparency on the use of algorithmic tools in government decision-making and has been subject to robust processes underpinning its design and development.

Article 22 of the UK GDPR requires compliance with additional rules to protect individuals if there is automated decision making that has legal or similarly significant effects on them. If data processing falls within this criteria, data controllers have additional requirements, including the need to give individuals information about the processing. The ATRS provides a standardised method of recording this information proactively and openly and thus is a useful communications tool public organisations can use to meet this transparency requirement. The government's response to consultation on the AI White Paper, published on 6th February, we announced that use of the ATRS will now become a requirement for all government departments, and the broader public sector in time. Mandating the ATRS in policy will move the default in government departments, and then the wider public sector, to publish ATRS records. This is a powerful shift, one which will enable the government to continue setting a standard for algorithmic transparency and driving public trust.

Accountability

I committed to write to explain the Government's position in relation to Baroness Jones' amendments 99 to 102, 105 to 108, and 167 because I ran out of time on the day this group of amendments was debated.

Amendments 99, 100 and 102 would make sure that when organisations are carrying out an assessment of high-risk processing under clause 20 of the Bill, they would be required to consider whether the processing involves automated decision-making that leads to significant decisions; and whether there is meaningful human involvement in those decisions from a suitably skilled individual. The amendments would also require organisations to consider any obligations under the Equality Act 2010 to prevent unlawful discrimination. I also want to reassure Baroness Kidron, who wanted more

clarity about data subject rights in this context, that controllers must continue to assess the risk to individual rights and freedoms when performing these assessments.

The government considers that it should not be necessary for the clause to specifically require organisations to consider these additional factors because it already requires controllers to consider any “risks to individuals” and describe “how the controller proposes to mitigate those risks”. This would clearly include any risks associated with automated decision-making, or risks that a processing activity might lead to unlawful discrimination.

Turning to amendments 105 to 108 which concern the circumstances in which data controllers should consult the ICO if an assessment of high-risk processing identifies potential risks to people. Amendments 105 and 107 would require organisations to consult with the Information Commissioner whenever potential risks to children were identified, while amendments 106 and 108 would maintain the current mandatory consultation requirements with the ICO when a risk assessment identifies potential high risks to any person. However, the ICO has found that mandatory consultation requirements do not, in fact, result in organisations sharing the outcomes of their risk assessments. Clause 21 of the Bill therefore replaces this requirement with the option of voluntary collaboration. To further encourage organisations to collaborate, the Bill also enables the ICO to take account of whether an organisation has approached it for consultation as a mitigating factor when considering any subsequent regulatory action.

Finally, amendment 167 seeks to confirm that if a data controller or data processor is compliant with the EU GDPR, they will also be considered compliant with the UK GDPR as amended by this Bill. While many organisations that are currently compliant with the EU GDPR will continue to be compliant with the new regime, this may not be the case for all. That is because this Bill introduces a small number of new requirements, such as requiring controllers to have a complaints handling process or to designate a Senior Responsible Officer if they conduct high risk processing or are a public body. The former will ensure complaints are dealt with effectively, while the latter should provide greater flexibility in managing data protection risks. However, both requirements will need to be adhered to in order to achieve compliance.

International data transfers

Lord Clement-Jones asked for information on the process to ensure that a third country is adequate. Lord Bassam also asked for an explanation on how data transfers are made to an overseas processor using the powers relied on by reference to new Section 73(4)(aa) of the 2018 Act. When conducting adequacy assessments for law enforcement purposes, as set out in the Bill, the Secretary of State is obliged to take into account the rule of law, respect for human rights, the existence and effective functioning of an authority with powers to enforce data subject rights, arrangements for judicial or non-judicial redress for data subjects, rules about the transfer of personal data to other jurisdictions, the constitution, traditions and culture of the country or organisation and any relevant international commitments. However, these factors are not exhaustive, and the Secretary of State can take into account any other factors considered relevant.

It is already a legal requirement for the Secretary of State to consult the ICO on all regulations being made under the UK GDPR and the Data Protection Act 2018, including when conducting adequacy assessments under the reformed Part 3, Chapter 5 International Transfer Regime framework. These assessments will therefore continue, as they do now, to involve active consultation and engagement with the ICO throughout the assessment process, including for the ICO to provide an opinion to the Secretary of State on the transfer of personal data to another country or international organisation. Lord Bassam has rightly concluded that the majority of the government amendments 110, 117-120, 122-129 and 131, have been made as consequential to the new section 73(4)(aa) of this Bill. This is because while such transfers are currently permissible under the current Data Protection Act 2018 (2018 Act), and it is within the intent of Part 3 of the 2018 Act, providing a bespoke route has resulted in a series of consequential amendments to ensure that the new provision works within the other existing transfer mechanisms and the broader framework set out in Chapter 5 of Part 3 of the 2018 Act.

Law enforcement controllers may continue to use the existing transfer mechanisms of adequacy, appropriate safeguards and special circumstances to transfer personal data to their contracted international processors. UK law enforcement authorities transfer data to international processors based on contracts required by section 59 of

the 2018 Act as they do for any other processor. We have made transitional provision so that existing contracts between controllers and their international processors will continue to stand if they would have previously fulfilled the requirements of a legal instrument containing appropriate safeguards in section 75(1)(a) of the 2018 Act.

Yours sincerely,

Viscount Camrose
Parliamentary Under Secretary of State at the
Department for Science, Innovation & Technology