Department for
Science, Innovation
& Technology

Rt Hon Sir John Whittingdale OBE MP
Minister for Data and Digital Infrastructure
Department for Science, Innovation
& Technology
100 Parliament Street
London SW1A 2BQ

www.gov.uk/dsit

22 September 2023

Dear Harriet,

The Government is grateful to the Joint Committee on Human Rights for providing much-needed Parliamentary scrutiny on this topic and for the recommendations put forward by the committee chair.

I appreciate the time the Committee took to consider the provisions in the Bill and the constructive suggestions you made. This document sets out a response from the Government to the letter.

Data reform is critical to ensuring Britain remains an innovative economy in a time of rapid technological change. By building on and modernising our existing foundations, while bringing together the best parts of data protection legislation from around the world, we can create an innovative, flexible and risk-based data protection regime. The Data Protection and Digital Information No.2 (DPDI) Bill allows for a bespoke UK model that will unlock the true benefits of data for our economy and for individuals lives, whilst continuing to ensure high data protection standards.

You expressed some concerns that our reforms would erode the fundamental data protection principles in the UK GDPR and weaken people's rights in respect of their data. I want to make it clear upfront that the UK remains firmly committed to maintaining high data protection standards and the proposals in the Bill are underpinned by this commitment. Even where the Bill includes measures to simplify the legislation or reduce unnecessary regulatory burdens on organisations, these measures are complemented by robust conditions and safeguards to protect the rights of individuals.

Your letter is a useful opportunity for me to hear your views on the Bill and I want to use this opportunity to assure you that the protection of personal data remains central to our proposed reforms. As set out in your letter, the DPDI (No.2) Bill ECHR Memorandum addressed many of the concerns expressed in the Committee's 2019 report; including concerns surrounding automated decision-making, national security exemption and regulation-making powers relating to customer data and business data (smart data).

Many organisations have welcomed the reforms including TechUK recognising them as "new, targeted package of reforms to the UK's data protection laws, which builds on ambitions to bring organisations clarity and flexibility when using personal data" and that the changes will "give companies greater legal confidence to conduct research, deliver basic business services and develop new technologies such as AI, while retaining levels of data protection in line with the highest global standards, including data adequacy with the EU. Chris Combemale, Chair of the DPDI Business Advisory Group and CEO of the Data & Marketing Association (DMA UK) has collaborated with the government throughout the Data Protection and Digital Information Bill (DPDI)'s development to champion the best interests of both businesses and their customers. Further stating the DAM is "confident that the bill should act as a catalyst for innovation and growth, while maintaining robust privacy protections across the UK – an essential balance which will build consumer trust in the digital economy." Where we have not accepted the conclusions and recommendations, we have outlined the existing or planned actions that are in progress to address the issues raised by the committee.

***Rights of Data Subjects***

The government agrees that it is important that data subjects have an ability to request access to information about them. The government does not expect the proposed reforms to lead to a substantial increase in requests being refused and contested. The current legislation sets out that any request from a data subject, including subject access requests, is to be responded to. The government is retaining this approach.

Clause 8 changes the threshold at which a controller can refuse or charge a reasonable fee for a request to be 'vexatious or excessive'. The government believes this change is proportionate, and controllers will be expected to demonstrate why the new 'vexatious or excessive' provision applies each time it is relied on. The government recognises the importance of the right of access - a clearer provision enables controllers to focus time and resources on responding to reasonable and proportionate requests.

Clause 8 also sets out specific parameters to emphasise the importance of proportionality when considering whether a request is 'vexatious or excessive'. The government expects that the new parameters are considered individually as well as in relation to one another, and a controller should consider which parameters may be relevant when deciding how to respond to a request.

***Clause 10***

Article 13 and 14 of the UK GDPR set out what information should be provided to data subjects at the point of collection when collected directly from the data subject or indirectly from another data controller. This includes information such as the identity and contact details of the controller and the purpose for processing, among other things.

Under the current legislation, when data is being collected indirectly, Article 14 gives controllers an exemption from providing the information required where doing so would require disproportionate effort. This recognises that there is a break in the link between the data subject and the controller in these cases which may make it impossible or extremely difficult to contact them to provide the required information.

During our engagement we also heard of examples in research, especially in the medical research field, where the same impossibility or extreme difficulty exists when further processing data, even when it was collected directly from data subjects.

*For example if researchers are studying a degenerative neurological condition and initially collected data from patients early on, they may discover years down the line that the data is also able to help them treat another medical condition. Due to the length of time, degree of pseudonymisation, and/or the nature of the condition these patients had, they may not be able - or it may no longer be appropriate for the researchers to contact them - to provide this information.*

To ensure that research such as this does not face barriers due to a requirement to provide information, most of which the data subject would have received at the point of data collection, Clause 10 introduces a disproportionate effort exemption into Article 13 which only applies when further processing personal data for scientific research purposes. Therefore, as outlined in the above example, this very limited exemption is required to address a very specific research issue.

The exemption is not without safeguards; Article 13 includes a non-exhaustive list of considerations to be taken into account when considering whether the 'disproportionate effort' exemption applies and data subjects will always have the option to refer to the ICO to review the controllers approach if they believe there is non-compliance.

Moreover, we have sought to improve transparency as part of the re-use reforms elsewhere in the Bill. Clause 6 makes explicit what was previously only implicit in the legislation, which is that if a controller has collected an individual's personal data in reliance on the lawful ground of consent (Article 6(1)(a) UK GDPR), they would need to get fresh consent if that data is being reused for research (amongst others) purposes unless an exemption applies.

This clarification is important as it will help ensure personal data is used appropriately and not in ways in which data subjects would not anticipate and which would damage public trust. This will help create a transparent framework that individuals can trust when they are sharing or re-using data and build a stronger research environment.

***Recognised legitimate interests***

As noted in the Department's European Convention on Human Rights Memorandum of 8 March 2023 ("the ECHR Memorandum"), if a legislative provision is capable of being operated in a manner which is compatible with Convention rights, in that it will not give rise to an unjustified interference with Article 8 rights in all or most cases, the legislation itself will not be incompatible with Convention rights (see para. 3 of the ECHR Memorandum).

When personal data is processed by a private body in reliance on the new Article 6(1)(ea) ground, Article 8 ECHR may or may not be engaged. Where it is, DSIT considers that it will not give rise to an unjustified interference in all or most cases since the controller is still obliged to consider the necessity of the processing. This incorporates a proportionality test whereby the controller must satisfy itself that the processing is no more intrusive than required to achieve the specific aim (see para. 13 of the ECHR Memorandum). Any processing of personal data that is disproportionate to the aim will not be made lawful by virtue of new A6(1)(ea). In addition, any personal data received by a public authority through a disclosure by a private body in reliance on new Article 6(1)(ea) will be specifically required to be processed in accordance with Article 8 ECHR, whether or not Article 8 was engaged when the personal data was processed by the private body.

As also noted in paragraph 13 of the ECHR Memorandum, save for consent (Article 6(1)(a) UK GDPR), all of the lawful grounds in Article 6(1) UK GDPR impose a necessity test without an additional legitimate interest balancing exercise. This includes processing necessary for the performance of a contract, for example (Article 6(1)(b) UK GDPR), which would be relied on by private bodies and organisations who are not bound to comply with Article 8 ECHR by the Human Rights Act 1998.

Sensitive personal data such as health records are additionally subject to the existing restrictions set out in Article 9 UK GDPR and must meet a condition for processing set out in Article 9(2), or in Schedule 1 to the Data Protection Act 2018

***Automated decision-making***

The rules related to solely automated decisions that have significant effects on individuals in the UK's data protection legal framework are ambiguous and complex. The result is that the available safeguards are rarely used effectively in practice. These rules are currently also framed as a general prohibition on automated decision-making of this nature, except where certain limited conditions apply (where necessary for contractual purposes; where such activity is required or authorised by law; or where a data subject has provided explicit consent). Our reforms will mean such automated decision-making is no longer restricted to three conditions.

Instead, reformed Article 22 sets out the safeguards that must apply, regardless of the lawful basis on which such activity is carried out. These safeguards preserve individuals' rights as contained in Article 22 UK GDPR, including the right to be provided with information about solely automated decisions that have significant effects on them; to contest and seek human review of any such decisions; and to have those decisions corrected when they have produced a wrongful outcome. As such, these reforms do not water down any of the protections offered under the current regime.

As set out at para.16- 26 of the ECHR Memorandum, Clause 12 although the reforms to the UK GDPR are likely to increase the level of automated decision-making of this nature, this will be from predominantly private organisations, as public bodies will generally rely on the lawful basis permitted in existing Article 22. The additional processing by private bodies will generally not raise ECHR concerns, because Article 8 ECHR will not be engaged when the controller is not an emanation of the State.

The Department therefore considers that any interference with either the freestanding Article 8 right or Article 14 ECHR (read with Article 8) complies with the principles of necessity and proportionality, as the measure provides comprehensive safeguards for data subjects and these reforms seek to enhance fairness, transparency, accountability, for automated decision-making of this nature. These safeguards now apply to all (both private and public) organisations to ensure they are implemented to prevent and minimise harmful outcomes and to facilitate the full enjoyment of the benefits that automated decision-making can provide.

The ICO, as the UK's body responsible for upholding information rights, can take direct action in cases where a clear and serious breach of the legislation has taken place. This can involve enforcement action, including monetary penalties for serious non-compliance. The government will work with the ICO to ensure appropriate guidance on these requirements is provided, including with regard to automated decision-making.

Finally, it is worth noting that the proposal associated with Automated Decision Making and Artificial Intelligence extends beyond the scope of the data protection framework. The government has published a White Paper setting out its context-specific approach to regulating AI. The White Paper sets out that fairness is one of the key principles, and AI systems should not undermine the legal rights of individuals or organisations, discriminate unfairly against individuals, or create unfair market outcomes. Other key principles set out in the White Paper, such as the accountability and governance principle, combined with the appropriate transparency and accountability principle, will be important enablers to promoting fairness in practice.

***Regulation making powers***

Clause 5(4) of the Bill provides that the Secretary of State can only add to the list of recognised legitimate interests where she considers it appropriate to do so, having regard to the rights and interests of individuals in relation to their personal data and, where relevant, the need to provide children with special protection. In addition, under clause 46 of the Bill, the Secretary of State would be required to consult the Information Commissioner and any other persons as the Secretary of State thinks appropriate before making any regulations (this requirement to consult is also true of the power in clause 12 discussed below). Any new regulations would also be subject to parliamentary scrutiny via the affirmative resolution procedure. Taken together, these safeguards will ensure that the regulation-making powers in clause 5 are used sparingly and in a way which respects the rights of individuals.

If the recognised legitimate interests list could only be updated using primary legislation, it could take many years to effect any necessary changes. This would not be desirable in cases where there was a pressing need to add a new processing activity to the list, for example to encourage responsible data sharing to protect the public or to fulfil other important objectives.

With respect to automated decision-making, the power will ensure that the safeguards remain fit for purpose as the adoption of automated decision-making grows. It is important to emphasise that the power in question enables the Secretary of State to amend or vary, or to introduce new safeguards for automated decision-making, but not to remove those that are introduced through this Bill. The power is similar to the existing power under section 14(7) DPA 2018, which is repealed as part of these reforms, to add or amend safeguards, but cannot be used to omit safeguards other than those which have been added through the exercise of the new power.

***Abolition of the Surveillance Camera Code and the offices of Surveillance Camera and Biometrics Commissioner***

Effective, independent oversight of the use of biometrics and surveillance camera systems is critical to public trust. This requires clear roles and responsibilities and consistent guidance. The consultation ahead of the Bill found that the current oversight framework is overlapping, complex and confusing for the public and the police, and supported the case for simplification set out in the DPDI Bill.

The Biometrics Commissioner's (BC) casework functions are transferring to the Investigatory Powers Commissioner's Office (IPCO). IPCO has expertise in carrying out similar types of casework and has more resilience as a much larger body. The BC's broader functions to review police retention of DNA and fingerprints overlap with the ICO's role, and the ICO is consulting on new guidance on

biometrics. The Forensic Information Database Strategy (FINDS) Board (the BC and the ICO both attend the Board) provides oversight of the use of the national police DNA and fingerprint databases and will continue to report annually to Parliament in this area, as will the ICO and IPCO on their statutory responsibilities. The Forensic Science Regulator (FSR) ensures that the provision of forensic science services (including biometrics) across the criminal justice system is subject to an appropriate regime of scientific quality standards, His Majesty's Inspectorate of Constabulary and Fire & Rescue Services independently assesses the effectiveness and efficiency of police forces in the public interest, and the College of Policing (CoP) sets standards, provides training, and shares good practice.

The Surveillance Camera Code covers police and local authorities' use of surveillance cameras, and reflects the principles set out in data protection, equalities, and human rights law, for example ensuring the way in which the surveillance camera system captures personal data is necessary, proportionate, legitimate, and transparent. The ICO regulates all organisations' data processing, including the use of surveillance cameras, and has produced its own video surveillance guidance covering similar ground to the Code. The ICO and Surveillance Camera Commissioner (SCC) both intervened in the *Bridges vs South Wales* live facial recognition (LFR) case, and both have issued guidance on LFR, as has the CoP. The Equalities and Human Rights Commission (EHRC) regulates compliance with the Human Rights and Equality Acts and, like the ICO, has enforcement powers. Where surveillance camera footage is used as part of evidence in a criminal investigation, this comes under the FSR's remit, who has included guidance on it in his Code of Practice.

As set out above there will continue to be extensive oversight in these areas, and we believe that the simplification in the DPDI Bill in this crowded space will lead to better oversight, and that was supported by the public consultation.

***Independence of the Information Commissioner's Office***

The Statement of Strategic Priorities will contain only the government's strategic priorities for data protection and is a transparent way to provide this helpful context for the ICO. Because it only contains the government's data protection priorities it is not necessary to follow an external consultation process and is in line with best practice for other such statements that are not intended to be directional. While the ICO must take the Statement into account when carrying out its functions, it is not required to act in accordance with it. This means the Statement will not be used in a way to direct what the ICO may and may not do. An additional process is not necessary as the draft Statement already requires parliamentary approval. The Statement must be laid in draft before Parliament before it can be designated and may not be designated if, within the 40 day period after it is laid, either House of Parliament resolves not to approve it.

Many of these reforms bring the ICO in line with its peers and it will remain accountable to Parliament in its supervision and enforcement of data protection regulation. We have worked closely with the Information Commissioner, who is supportive of these reforms.

We are committed to maintaining the ICO's independence, and the Information Commissioner himself made clear in giving his evidence to the Public Bill Committee that he feels that our reforms are compatible with that. He stated "No, I do not believe it will undermine our independence at all. What I think it will do is to further enhance and promote our accountability, which is very important". In line with the comments from the Information Commissioner, I would like to assure you of the Government's commitment to regulatory independence and consistency across different regulatory regimes.

Alongside the statement of strategic priorities the proposed reforms to the statutory codes, we have set out a broad range of reforms, including requirements for published impact assessments and consultation with panels of experts, to introduce greater accountability, robustness and transparency for the ICO. The expert panels the bill requires will help the ICO assess fast-evolving uses of data and new technologies at an early stage of the process, ensuring final approval of statutory codes can be swift. Taken together, we expect these reforms to ensure the ICO produces effective and helpful statutory codes to support data controllers in understanding their responsibilities in complying with the law.

I appreciate all the ongoing effort to ensure the protection of personal data is maintained and I welcome the Committee's ongoing interest in this important issue.

With best wishes,

Rt Hon Sir John Whittingdale OBE MP
**Minister for Media, Tourism and Creative Industries**