Author: Jeni Tennison **Date:** 14th May 2023

Data Protection and Digital Information (No.2) Bill

Written evidence from CONNECTED BY DATA

About CONNECTED BY DATA

We campaign to give communities a powerful say in decisions about data to create a just, equitable and sustainable world through collective, democratic and open data governance. We are a non-profit company limited by guarantee founded in March 2022 with funding from the Shuttleworth Foundation, and a staff team of seven with expertise on data, AI and democratic participation.

Key points

- Data is a driver of power and progress in modern democratic societies. It has become the medium of relationships between citizens and the state, and between consumers and companies, as well as being the foundation of AI and automated decision making. How it's regulated affects almost every aspect of our work and lives.
- The Data Protection and Digital Information (No.2) Bill removes important citizen data rights and undermines existing safeguards, parliamentary sovereignty, and democratic governance of data. It misses a critical opportunity to build public confidence in technology and innovation and deliver business and public benefit.
- At the same time, the Bill's business benefits are minimal and its changes provoke the risk of a politicised decision on data adequacy by the European Commission at a time of already strained relations with the EU. Most SMEs are already exempt from the most costly aspects of GDPR. The largest companies will achieve negligible savings as they need to support new and multiple regimes. The Bill's impact on public trust will counterproductively hamper data sharing and technology adoption.
- Amendments are needed to give citizens and communities a powerful say through a combination of meaningful individual rights, powerful collective representation, and proper democratic scrutiny and accountability. This will enable agile and context-aware regulation, protect citizens, and foster sustainable and responsible innovation.

Within this written evidence, the background provides evidence and rationale for a set of amendment areas, organised topically. The amendment detail that follows provides a clause-by-clause description of potential amendments.

Background

Discussions we convened across civil society in September, December, and March identified multiple aspects of this Bill that require scrutiny and revision. Reform to data regulation is certainly needed, but there are concerns across civil society that the Bill as it stands takes us backwards rather than supporting the foundations of a sustainable and fair digital economy.

The Bill's changes to the UK's data protection regime raises the prospect of a politically charged decision on **data adequacy** by the European Commission. The cost of losing data adequacy, which eases data transfers between the UK and the EU, is estimated as between £1 billion and £1.6 billion and would outstrip any business benefits to this Bill. Adequacy is threatened by the Bill's changes to the international data transfer regime, reduced independence of the ICO, and Secretary of State (SoS) powers. While these changes may not pose an immediate threat to the adequacy decision, they create instability and uncertainty: adequacy becomes dependent on trade deals and how the SoS wields their powers.

Independent analysis suggests the government's estimates of **savings for businesses** are highly inflated; any benefits that do arise from reduced regulatory requirements would mostly be felt by larger companies. Even those companies may continue to comply with GDPR to avoid the costs of changes to established practice, compliance with multiple regimes, and the knock-on effects of reduced public trust from adopting reduced standards. Among this uncertainty for business, it is clear that citizen and consumer data rights are being undermined by the Bill, which increases the barriers to exercising those rights and upholding safeguards.

Challenges of modern data processing

Our focus at **CONNECTED** BY **DATA** is on addressing the outdated assumptions that make data protection law unfit for purpose when regulating contemporary data processing. Dr Salome Viljoen's seminal paper "A Relational Theory of Data Governance" describes how modern big data processing techniques, including machine learning, mean that decisions that affect someone can be made based largely on data about other people. There are two implications that are vital for lawmakers to grasp.

First, it is becoming increasingly common – across healthcare, employment, education and digital platforms – for **algorithms created through training on one set of people to be used to reach conclusions about another set**. Ofqual's use of past exam results to grade current students during the pandemic is an example that attracted widespread acrimony. Amazon's AI recruitment tool that filtered out applications from women is another. Decisions can be made based on very little and seemingly innocuous information – the first part of your postcode; whether you liked a particular tweet. You don't need to provide sensitive information for a data-based or algorithmic decision to have a significant impact on you.

Second, as algorithms and AI permeate business and government operations, personal data is also used to make **decisions that affect whole groups of people** rather than identified individuals. Routes of gritting lorries, buses or police patrols; food prices and energy tariffs; the allocation of resources towards infrastructure such as schools and libraries – algorithmic decision-making can increase the efficiency with which these decisions are made. But they also have consequences for the people and communities who are affected by them, and frequently fall hardest on under-privileged groups.

Further, there is evidence that data collection, use and distribution can have both **positive and negative externalities**: impacts on the economy, society, and the environment. What and how data gets shared can support or stifle market competition; encourage or suppress innovation. What data is collected and how it is used can lead to discriminatory outcomes, undermine trust

in public institutions, improve public health, and influence democratic participation. Data can help us to Net Zero; but its storage and processing also consumes water and produces carbon emissions.

Modern, agile, ethical and context-aware data governance practices consider the impacts of data collection and processing beyond data subjects. Legislation should enable, encourage and enforce the adoption of these best-in-class data governance practices that ensure the full set of interests of those affected by data collection and use are heard and protected. This would mitigate harms and gain the public trust critical for advancing data-driven innovation, particularly for public benefit. To achieve this aim, an empowered public voice around data needs to be at the heart of this legislation. In practice this requires a combination of meaningful individual rights, powerful collective voice, and proper democratic scrutiny and accountability.

Amendment areas

We would like to see amendments in the following areas. These are geared towards the goal of modernising the UK's data protection regime to better meet the demands of a fast-moving and unpredictable technology landscape, so that socially and economically useful innovation is supported, and not undermined by mistrust, scandal and unproductive uses of powerful technology.

In each area we lay out the specific amendments we would like to see made, with detail provided at the end, and then the amendment areas proposed we would support.

Meaningful individual rights and controls

The Bill needs to be amended to bolster individual rights and recognise the power imbalance between individuals and private and public organisations that collect and use data.

Decision subjects rights

There is a disconnect between the traditional notion of "data subject" and the much larger group who are affected by automated decision-making. Data governance scholars – for example, University of Oxford's Reuben Binns in his article "Algorithmic Accountability and Public Reason" – have therefore come to call the subjects of algorithmic decision making "decision subjects".

For example, consider the following scenarios:

- A profiling company uses data about the mental health of some volunteers (special category data) to construct a model that predicts mental health conditions based on people's social media feeds (not special category data), and from that gives an estimate of how much time people are likely to take off work. A recruitment agency uses this model to assess candidates and weed out those who are likely to have extended absences. The recruitment agency never uses any special category data about the candidates directly in their automated decision-making.
- A person who has locked down their web browser such that it doesn't retain tracking cookies or share information such as their location visits an online service. The online service has collected data about the purchasing patterns of similarly anonymous users, and

knows they are willing to pay more for the service, so automatically provides a personalised price on that basis. No personal data about the purchaser is used in determining the price they are offered.

- An electricity company gets data from the subset of their customers who have smart devices in their home about the details of their home energy consumption. Based on this data, they automatically adjust the times of day when they offer cheaper tariffs. Everyone who uses the electricity company is affected, whether data about their energy consumption patterns was used in the decision or not.

These scenarios illustrate that an individual should have rights wherever they are subject to an automated decision that has a legal or similarly significant effect on them, not only when personal data is held about them.

Many of the rights and interests of decision subjects are protected through other pieces of legislation: the Equality Act 2010, Human Rights Act 1998, Consumer Rights Act 2015 and so on. What is not covered by other items of legislation is how data can be used in *automated* decisions, and the rights of decision subjects to be informed about, control and seek redress around automated decisions when they have a significant effect on them.

Therefore, in **Clause 11**, the Bill should give rights to the people affected by an automated decision (decision subjects), not just those who provide data (data subjects). We therefore support **Amendment NC12** to introduce a definition of decision subjects but recommend a broad definition of decision subjects as "living individuals for whom a decision is a significant decision".

If such an amendment is adopted, the legislation should also::

- have a requirement for decision subject rights and interests to be considered when the SoS creates new recognised legitimate interests (**Clause 5**)
- encourage codes of conduct to make provision with regard to decision subjects (**Clause 19**)
- ensure the ICO protects the rights of decision subjects (**Clause 27**)
- have a requirement for codes of practice to have regard to decision subjects (**Clause 29**)
- enable decision subjects to complain about automated decision-making (**Clause 39**)

Other amendments areas we support

We would also support amendments to see limits on the ability of organisations to avoid or delay responding to data subjects by classifying their requests as vexatious or excessive (**Clause 7**).

Powerful collective voice

The Bill needs to recognise that data protection is not only about individual privacy and emphasise our collective interests such as equality, education, access to public services, strong democratic institutions, a sustainable environment, and economic growth and innovation.

The public interest in data processing

The collection and use of data can have far-reaching impacts – both positive and negative – and not just on the individuals identifiable within a given dataset. When organisations weigh up

different interests to make decisions about what and how data can be collected and how it is processed, they should always include consideration of these wider impacts of data on people, communities, society, equality, and the environment. Allowing this to be a factor would both avoid wider harms and enable public good uses of data.

Amendments should require decision makers to consider the public interest when:

- organisations carry out balancing tests for legitimate interest uses of data (**Clause 5**)
- the Secretary of State (SoS) creates new recognised legitimate interests (**Clause 5**)
- organisations assess purpose limitation on further processing of personal data (**Clause 6**)
- assessing the need for organisations to keep records of data processing (**Clause 15**)
- organisations carry out assessments of high risk processing (**Clause 17**)
- the ICO creates codes of practice (**Clause 29**)
- the Secretary of State or Treasury require the provision of customer data (**Clause 62**)
- the Secretary of State or Treasury require the provision of business data (**Clause 64**)

Consultation during assessments of high risk processing

In **Clause 17**, the Bill replaces data protection impact assessments (DPIAs) with assessments of high risk processing. In doing so, it removes a key ability for those likely to be affected by data processing to be consulted in the process.

Best practice in data governance includes consultation and engagement with the people and communities who are affected by data, algorithms and AI, to build fairness, trust and legitimacy of data processing. Multiple reports emphasise the importance of public participation in data governance, including:

- the UNESCO "Recommendation on the Ethics of Artificial Intelligence"
- the Data Justice Lab's report "Civic Participation in the Datafied Society: Towards Democratic Auditing?"
- the Ada Lovelace Institute's reports "Rethinking data and rebalancing power", "Who cares what the public think?" and "Participatory Data Stewardship"
- the TUC's report "People Powered Technology"
- the Institute for the Future of Work's "Good Work Algorithmic Impact Assessment"
- the Goldacre Review "Better, broader, safer: using health data for research and analysis"

Engagement with affected stakeholders during impact assessment can help to:

- avoid and mitigate **harms** that may be overlooked by developers, procurers and controllers of technology
- identify additional constraints, **safeguards** and areas for ongoing monitoring that should be put in place
- build engagement and **trust** between data controllers and data subjects or the public at large, improving adoption and reducing the chance of backlashes
- build the **confidence** of data controllers in the legitimacy of the data processing they wish to carry out by better understanding public expectations and social licence
- support **risk management** as data controllers better understand potential harms from data processing and can identify and manage potential reputational risks

The advantages of consultation are particularly relevant when data subjects cannot opt out of data processing, for example because it is not carried out under the *consent* legal basis, or it would be impractical to secure consent for additional data processing. Consultation also plays a critical role when *consent* is limited because of the power relationship between controllers and individuals, for example in employment contexts, or when data is processed to deliver critical public services. Indeed, in these circumstances, there are no other mechanisms for the expectations and interests of data subjects to be heard and understood. Consultation is also essential when the people and communities other than data subjects are affected by data processing, as described above.

An amendment is therefore needed to reinstate and enhance consultation with individuals who are likely to be affected by high-risk data processing, or their representatives, during assessment processes (currently repealed by Clause 17(3)(f)).

Meaningful consultation at this stage will improve the deployment of technology by preventing harms, enhancing confidence, and reducing friction at later stages.

Other amendment areas we support

The Bill disproportionately places the burden of protecting rights and due process onto individuals, a significant practical and power imbalance when set against government bodies or companies. Advancing collective interests requires collective representation.

An amendment is needed to enable representative organisations – such as unions or consumer rights bodies – to act on behalf of data and/or decision subjects. We therefore support **Amendment NC10** to which introduces a new Clause in the Bill that would would require the Secretary of State to exercise powers under Section 190 of the Data Protection Act 2018 to allow organisations to raise data breach complaints on behalf of data subjects generally, in the absence of a particular subject who wishes to bring forward a claim about misuse of their own personal data.

Proper democratic scrutiny and accountability

Recent uses of data have led to low levels of trust which will hamper the progress of innovation and technology adoption. The bill needs to address this.

Publication of assessments of high risk processing

The Bill provides an opportunity to improve accountability and bolster trust by mandating transparency from government and businesses through the publication of their assessments of high-risk processing, through inserting such a requirement in **Clause 17**.

The ICO's guidance on Data Protection Impact Assessments (DPIAs) states:

> Although publishing a DPIA is not a requirement of UK GDPR, you should actively consider the benefits of publication. As well as demonstrating compliance, publication can help engender trust and confidence. We would therefore recommend that you publish your DPIAs, where possible, removing sensitive details if necessary.

Transparency accorded through the publication of impact assessments is particularly important for public bodies, and both summaries and links to impact assessments are included as part of

the Algorithmic Transparency Recording Standard developed by the Central Digital and Data Office and the Centre for Data Ethics and Innovation.

Despite this advice and guidance, very few organisations currently publish their Data Protection Impact Assessments. Transparency would support **informed consent** and **public debate** about data processing practices, and understanding of the mitigation mechanisms organisations put in place to protect people's privacy and other rights, interests and freedoms. This can build appropriate **trust and confidence** in data processing, and **early detection, accountability and correction** where those mechanisms are not sufficient. It can also help to **inform regulators** about the landscape, so that they are better able to **tailor guidance and interventions** and adapt more quickly to a fast-changing data and technology environment.

Data Protection Impact Assessments (or an assessment of high risk processing as these are now termed under the Data Protection and Digital Information (No. 2) Bill) are only required to be carried out when "a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a **high risk** to the rights and freedoms of natural persons" (our emphasis). Publication is a small additional step for organisations who decide, following the assessment, to go ahead with data processing that poses a high risk to people's rights and freedoms.

Other amendment areas we support

We also support amendments to ensure the **independence of the ICO** from the Government and to enhance the transparency and regular auditing of the public sector's use of algorithms. Alongside this, we support those that **limit Henry VIII powers** that enable the Government to write its own rules, and enhance the role of participatory and deliberative processes around data. We are particularly concerned by the lack of consultation on the new **'recognised' legitimate interests** within the Bill (**Clause 5**), and the ability of the SoS to add to this list without scrutiny

Priority amendment detail

No.	Clause	Lines	Amending	Change	Rationale
Clause 5 – Lawfulness of processing					
Require data controllers to consider the public interest when processing personal data under the 'legitimate interest' basis					
1	5(2)	page 6, line 18	UK GDPR Art. 6(1)	after point (b) insert: (ba) in point (f) — after "third party" insert "or in the public interest" — after "child" insert ","or the public interest"	Clause 5(2) amends UK GDPR Article 6(1), which defines the lawful bases for data processing. This amendment alters the "legitimate interests" lawful basis defined in point (f) of Article 6(1) so that it reads "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party or in the public interest, except where such 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, or the public interest." The first insertion enables the public interest to be valid legitimate interest and matches the ICO guidance on the applicability of the legitimate interests lawful basis which states "A wide range of interests may be legitimate interests. They can be your own interests or the interests of third parties, and commercial interests **as well as wider societal benefits**." (our emphasis), but provides clarity about this point in the legislation itself. The second insertion also ensures the public interest is considered on the other side of the balancing test, as a factor that may weigh against the processing of personal data.

No.	Clause	Lines	Amending	Change	Rationale
Require the SoS to have regard to decision subject interests when creating new recognised legitimate interests					
2	5(4)	page 6, line 35	UK GDPR Art. 6(7)	after point (a), insert: (aa) the interests and fundamental rights and freedoms of decision subjects as defined in Article 22A, and	Clause 5(4) inserts sub-paragraphs (5)-(10) into Article 6 of the UK GDPR, providing for 'recognised legitimate interests' as a legal basis for data processing, and enabling the Secretary of State to create new recognised legitimate interests by regulations. The new Article 6(7) places conditions on when the Secretary of State may make these regulations, including having regard to data subject interests and fundamental rights and freedoms. This amendment requires the Secretary of State to also have regard to decision subject interests and fundamental rights and freedoms when creating new recognised legitimate interests. This means the Secretary of State will have to consider the kinds of decisions that might be made using that data.
Require the SoS to consider the public interest when defining new recognised legitimate interests					
3	5(4)	page 6, line 37	UK GDPR Art. 6(7)	after point (b), insert: (c) the public interest	Clause 5(4) inserts into Article 6 of UK GDPR paragraphs that allow for the Secretary of State to define new recognised legitimate interests. The new Article 6(7) lists the factors that the SoS must have regard to when doing so. This amendment adds the public interest to that list (alongside the interests of data subjects and the need to provide children with special protection with regard to personal data about them).

No.	Clause	Lines	Amending	Change	Rationale
Clause 6 – The purpose limitation					
Require data controllers to consider the public interest when assessing the purpose limitation on further processing of personal data					
4	6(5)	page 8, line 19	UK GDPR Art. 8A(2)	in point (d), after "data subjects" insert "and the public interest"	Clause 6(5) inserts a new Article 8A (Purpose limitation: further processing) into UK GDPR, which describes when a data controller can use personal data for purposes other than those for which it was originally collected. Article 8A(2) lists factors that the person making this assessment has to take into account. This amendment changes point (d) in this list to read: "the possible consequences of the intended processing for data subjects and the public interest;". It ensures that wider public interest reasons for or against the further processing of personal data are taken into account in the assessment.
Clause 11 – Automated decision-making					
Define "decision subject" in the context of automated decision-making					
5	11	page 18, line 1 to page 22, line 17		replace "data subject" with "decision subject" throughout	Rights surrounding automated decision-making should be conferred on decision subjects rather than data subjects.
6	11(1)	page 18, lines 8-16	UK GDPR Art. 22A(1)	define "decision subject" as "living individuals for whom a decision is a significant decision"	This definition covers those on whom an automated decision has a legal or similarly significant effect (as defined earlier in Clause 11).

No.	Clause	Lines	Amending	Change	Rationale
7	11(1)	page 18, line 23	UK GDPR Art. 22B(1)	after "special categories of personal data referred to in Article 9(1)", add "(whether relating to the decision subject or otherwise)" so that the paragraph reads: 1. A significant decision based entirely or partly on special categories of personal data referred to in Article 9(1) (whether relating to the decision subject or otherwise) may not be taken based solely on automated processing, unless one of the following conditions is met.	The new Article 22B provides additional safeguards when a decision is based on special categories of personal data (such as gender, race, or political affiliation) as there is more risk of harm in these cases. The amendment clarifies that these additional safeguards apply even if the special category personal data used in the decision relates to people other than the decision subject. This addresses the situation where a decision subject is profiled through non-special category data about them being combined with special category data about other people.
8	11(1)	page 19, line 5	UK GDPR Art. 22C(1)(a)	after "personal data", add "(whether relating to the decision subject or otherwise)" so the sub-paragraph reads: a. based entirely or partly on personal data (whether relating to the decision subject or otherwise), and	The new Article 22C provides additional safeguards around decisions based solely on automated processing. The amendment clarifies that these additional safeguards apply even if the personal data used in the decision relates to people other than the decision subject. This addresses the situation where a decision is made that affects a group of people based on personal data about a subset of that group or a different group entirely.
9	11(3)	page 20, lines 4-16	DPA 2018 S. 50A(1)	define "decision subject" as "living individuals for whom a decision is a significant decision"	As above.

No.	Clause	Lines	Amending	Change	Rationale
10	11(3)	page 20, line 20	DPA 2018 S. 50B(1)	after "sensitive personal data", add "(whether relating to the decision subject or otherwise)" so that the paragraph reads: (1) A significant decision based entirely or partly on sensitive personal data (whether relating to the decision subject or otherwise) may not be taken based solely on automated processing, unless one of the following conditions is met.	As above.
11	11(3)	page 20, line 29	DPA 2018 S. 50C(1)(a)	after "personal data", add "(whether relating to the decision subject or otherwise)" so that the paragraph reads: (a) based entirely or partly on personal data (whether relating to the decision subject or otherwise), and	As above.

No.	Clause	Lines	Amending	Change	Rationale
Clause 15 – Duty to keep records					
Require data controllers to consider risks to the public interest when keeping records of personal data processing					
12	15(4)	page 29, line 28	UK GDPR Art. 30A(1)	in point (a), after "individuals" insert "or to the public interest"	Clause 15(4) inserts a new Article 30A (Records of processing of personal data) into UK GDPR, which describes which records data controllers and data processors need to keep. Article 30A(1)(a) defines the circumstances under which records need to be kept. This amendment changes point (a) in this list to read: "paragraphs 2 to 4, 8 and 9 apply to a controller that carries out processing of personal data which, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of individuals or to the public interest, and". It ensures that records must be kept when processing data is likely to result in a high risk to the public interest, even if it doesn't impact on the rights and freedoms of individuals. Examples might be data processing that has a high risk of environmental damage, or to trust in democratic institutions.
13	15(4)	page 30, line 36	UK GDPR Art. 30A(9)	in point (b), after "individuals" insert "or to the public interest"	Clause 15(4) inserts a new Article 30A (Records of processing of personal data) into UK GDPR, which describes which records data controllers and data processors need to keep. Article 30A(9)(b) describes what controllers and processors should take into account when deciding what records to keep. This amendment changes point (b) in this list to read: "the risks for the rights and freedoms of individuals or to the public interest arising from that processing, including the likelihood of risks arising and their severity, and". It ensures that risks to the

No.	Clause	Lines	Amending	Change	Rationale
					public interest are taken into consideration when controllers and processors determine which records to keep.
14	15(9)	page 32, line 3	DPA 2018 S. 61A(8)	in point (b), after "individuals" insert "or to the public interest"	Clause 15(9) inserts a new Section 61A (Records of processing of personal data) into the DPA 2018, which describes which records data controllers and data processors need to keep. Section 61A(8)(b) describes what controllers and processors should take into account when deciding what records to keep. This amendment changes point (b) in this list to read: "the risks for the rights and freedoms of individuals or to the public interest arising from that processing, including the likelihood of risks arising and their severity, and". It ensures that risks to the public interest are taken into consideration when controllers and processors determine which records to keep.
Clause 17 – Assessment of high risk processing					
Require data controllers to consider the public interest when carrying out assessments of high risk processing					
15	17(3)(b)	page 32, line 17	UK GDPR Art. 35(1)	replace point (b) with: (b) in paragraph 1, for "natural persons" substitute "individuals or to the public interest",	Clause 17(3) amends Article 35 (data protection impact assessment) of the UK GDPR, to describe a new regime of assessments of high risk processing. Article 35(1) describes the circumstances under which a data protection impact assessment (now assessment of high risk processing) should occur. Clause 17(3)(b) simply replaces "natural persons" with "individuals" in this paragraph. This amendment adds "or to the public interest" to the existing amendment. UK GDPR Article 35(1) would then read:

No.	Clause	Lines	Amending	Change	Rationale
					(b) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of individuals or to the public interest, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. This requires assessments to be carried out not only when there is a risk for individuals, but when there are wider risks to the public interest from data processing, such as to the economy, society or the environment.
16	17(3)(d)	page 32, line 27	UK GDPR Art. 35(7)	after point (c), insert: (b) an assessment of risks and benefits to the public interest, including impacts on equality	Clause 17(3) amends Article 35 (data protection impact assessment) of the UK GDPR, to describe a new regime of assessments of high risk processing. Clause 17(3)(d) replaces Article 35(7) which describes the content of those risk assessments. This amendment adds a new point (d) to Article 35(7), meaning that as well as assessing the risks to individuals, data controllers need to include an assessment of wider risks and benefits to the public interest. It calls out the need for equality impact assessments in particular.
17	17(4)	page 33, line 8	UK GDPR Art. 57(1)(k)	after "individuals", insert "or to the public interest"	Clause 17(4) amends Article 57 (tasks) of the UK GDPR, which lists tasks for the Information Commissioner, to include a task to provide guidance about the kinds of data processing that are

No.	Clause	Lines	Amending	Change	Rationale
					high risk, and therefore when an assessment should be carried out. This amendment changes this to read: "produce and publish a document containing examples of types of processing which the Commissioner considers are likely to result in a high risk to the rights and freedoms of individuals or to the public interest (for the purposes of Articles 27A, 30A and 35);"." It means that this guidance should also describe when data processing poses a high risk to the public interest.
18	17(7)	page 33, lines 15-17	DPA 2018, S. 64(1)	substitute point (b) with: (b) in subsection (1), — after "natural persons", insert "or to the public interest" — for "a data protection impact assessment" substitute "an assessment of the impact of the envisaged processing operations",	Clause 17(7) amends Section 64 (data protection impact assessment) of the DPA 2018, to describe a new regime of assessments of high risk processing. Section 64(1) describes the circumstances under which a data protection impact assessment (now assessment of high risk processing) should occur. Clause 17(7)(b) replaces "a data protection impact assessment" with "an assessment of the impact of the envisaged processing operations on the protection of personal data" in this paragraph. This amendment adds consideration of the public interest to the existing amendment. DPA 2018 Section 64(1) would then read: (1) Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals or to the public interest, the controller must, prior to the processing, carry out an assessment of the impact of

No.	Clause	Lines	Amending	Change	Rationale
					the envisaged processing operations ~~on the protection of personal data~~. This requires assessments to be carried out not only when there is a risk for individuals, but when there are wider risks to the public interest from data processing, such as to the economy, society or the environment.
19	17(7)(d)	page 33, line 26	DPA 2018 S. 64(3)	after point (c), insert: (d) an assessment of risks and benefits to the public interest, including impacts on equality	Clause 17(7) amends Section 64 (data protection impact assessment) of the DPA 2018, to describe a new regime of assessments of high risk processing. Clause 17(7)(d) replaces Section 64(3) which describes the content of those risk assessments. This amendment adds a new point (d) to Section 64(3), meaning that as well as assessing the risks to individuals, data controllers need to include an assessment of wider risks and benefits to the public interest. It calls out the need for equality impact assessments in particular.
Clause 17 – Assessment of high risk processing					
Require data controllers to consult with individuals likely to be affected by the intended processing during risk assessment					
20	17(3)	page 32, line 32	UK GDPR Art. 35(9)	replace point (f) with: (f) in paragraph (9) — remove "Where appropriate," — for "data subjects" substitute "individuals likely to be affected by the intended processing"	Clause 17 amends UK GDPR Article 35, which defines how data controllers go about conducting Data Protection Impact Assessments (DPIAs) and replaces them with assessments of high risk processing. Clause 17(3)(f) removes the existing Article 35(9), which encourages data controllers to seek the views of data subjects on the intended processing. This amendment reverses that change, and instead changes

No.	Clause	Lines	Amending	Change	Rationale
					the wording of Article 35(9) so that it reads: "~~Where appropriate,~~ The controller shall seek the views of ~~data subjects~~ individuals likely to be affected by the intended processing or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations." Removing "Where appropriate," removes uncertainty about when consultation should take place. Replacing "data subjects" with "individuals likely to be affected by the intended processing" ensures that the interests of non-data-subjects can be represented in the consultation.
Require data controllers to publish assessments of high risk processing					
21	17(3)	page 32, line 32	UK GDPR Art. 35	after point (f) insert: (g) after paragraph (9) insert – "(9A) The controller shall publish the document described in paragraph 7, redacted where necessary for the protection of commercial or public interests or the security of processing operations."	Clause 17(3) amends UK GDPR Article 35, which defines how data controllers go about conducting Data Protection Impact Assessments (DPIAs) and replaces them with assessments of high risk processing. This amendment causes a new paragraph (9A) to be inserted into Article 35, requiring the publication of assessments of high risk processing but allows for reasonable redactions.

No.	Clause	Lines	Amending	Change	Rationale
Clause 19 – Law enforcement processing and codes of conduct					
Encourage the creation of codes of conduct that define information provided to decision subjects and the exercise of their rights					
22	19(6)	page 35, lines 11-12	DPA 2018 S. 68A(4)	Replace sub-paragraphs (c) and (d) with: (c) the information provided to the public and to data subjects and decision subjects as defined in Section 50A; (d) the exercise of the rights of data subjects and decision subjects as defined in Section 50A;	Clause 19(6) inserts a new Section 68A to the Data Protection Act 2018 which requires the Commissioner to encourage public bodies to produce codes of conduct that take account of the specific context of different sectors. S. 68A(4) lists the kinds of provisions these codes of conduct may contain. This amendment encourages the creation of codes of conduct that define information provided to decision subjects and the exercise of the rights of decision subjects, as well as data subjects.
Clause 27 – Duties of the Commissioner in carrying out functions					
Require the Information Commissioner to have regard to the interests of decision subjects					
23	27(3)	page 47, line 27	DPA 2018 S. 120A(a)	after "data subjects,", insert "decision subjects as defined in Section 50A", so that the paragraph reads: (a) to secure an appropriate level of protection for personal data, having regard to the interests of data subjects, decision subjects as defined in Section 50A, controllers and others and matters of general public interest, and	Clause 27(3) inserts a new Section 120A to the Data Protection Act 2018 which defines the principal objective of the Information Commissioner. This amendment makes explicit that the Information Commissioner should have regard to the interests of decision subjects as well as data subjects.

No.	Clause	Lines	Amending	Change	Rationale
Clause 29 – Codes of practice for the processing of personal data					
Require the Information Commissioner to consider the public interest when creating new codes of practice					
24	29(2)	page 53, line 22	DPA 2018 S. 124A(7)	after "legislation", insert ", and general public interest"	Clause 29(2) inserts a new Section 124A (Other codes of practice) into the DPA 2018, to describe codes of practice that the Information Commissioner might be required to produce. Section 124A(7) defines "good practice in the processing of personal data". This amendment slightly changes that definition, so that it reads: ""good practice in the processing of personal data" means such practice in the processing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, including compliance with the requirements of the data protection legislation, and general public interest;" This ensures that Commissioner takes into account general public interest when creating codes of practice.
Require the Information Commissioner to consult with decision subjects when preparing codes of practice					
25	29(2)	page 53, line 11	DPA 2018 S. 124A(4)	replace sub-paragraph (c) with: (c) decision subjects as defined in Section 50A; (d) persons who appear to the Commissioner to represent the interests of data subjects or decision subjects.	Clause 29(2) inserts a new Section 124A to the Data Protection Act 2018 which requires the Information Commissioner to prepare codes of practice when required to do so by the Secretary of State. Section 124A(4) lists the people who should be consulted by the Information Commissioner when preparing these codes of practice.

No.	Clause	Lines	Amending	Change	Rationale
					This amendment adds decision subjects and those who represent their interests to the list of people to be consulted.
Clause 39 – Complaints to controllers					
Enable decision subjects to make complaints to data controllers					
26	39(2)	page 67, lines 34-35	DPA 2018 S. 164A	replace the title and paragraph (1) with: **"164A Complaints by data and decision subjects to controllers** (1) A data subject or decision subject may make a complaint to the controller if the data subject or decision subject considers that, in connection with personal data relating to the data subject or decisions related to the decision subject, there is an infringement of the UK GDPR or Part 3 of this Act.	Clause 39(2) inserts a new Section 164A to the Data Protection Act 2018 which requires data controllers to enable data subjects to make complaints to them. This amendment enables decision subjects to make complaints under this clause as well.
Clause 62 – Power to make provision in connection with customer data					
Require the SoS and Treasury to consider the public interest when making Smart Data regulations					
27	62(4)	page 87, line 12	-	after point (e), insert: (f) the likely effect on matters of public interest, including equality	Section 62 (Power to make provision in connection with customer data) gives the SoS or the Treasury the power to require data holders to provide customer data to customers or third parties. Section 62(4) lists the factors that the SoS or the Treasury should have regard to when they make regulation under this provision, including the likely effects on current and

No.	Clause	Lines	Amending	Change	Rationale
					future customers, data holders, SMEs, innovation and competition. Experience with Open Banking has shown that the approach to Smart Data initiatives can have both positive and negative impacts on wider considerations such as financial inclusion, and on non-private sector actors, such as researchers or civil society organisations. This amendment requires the SoS or Treasury to also have regard to the likely effect on matters of public interest when making such provisions, and calls out impacts on equality in particular.
Clause 64 – Power to make provision in connection with business data					
Require the SoS and Treasury to consider the public interest when making Smart Data regulations					
28	64(3)	page 89, line 22	-	after point (e), insert: (f) the likely effect on matters of public interest, including equality	Section 64 (Power to make provision in connection with business data) gives the SoS or the Treasury the power to require data holders to publish or provide business data. Section 62(3) lists the factors that the SoS or the Treasury should have regard to when they make regulation under this provision, including the likely effects on current and future customers, data holders, SMEs, innovation and competition. Experience with Open Banking has shown that the approach to Smart Data initiatives can have both positive and negative impacts on wider considerations such as financial inclusion, and on non-private sector actors, such as researchers or civil society organisations.

No.	Clause	Lines	Amending	Change	Rationale
					This amendment requires the SoS or Treasury to also have regard to the likely effect on matters of public interest when making such provisions, and calls out impacts on equality in particular.