Public Law Project

Public Law Project House of Commons second reading briefing on the Data Protection and Digital Information Bill

August 2022

Summary and Recommendations

1. We live in an increasingly data-driven world. Social media giants, insurance companies and governments collect and process personal data on an ever-increasing scale. Relatedly, automated decision-making is also on the rise. Personal data is fed into automated systems, which are now used to make decisions that would traditionally have been made by human beings: decisions about immigration, welfare benefits, and policing, to name a few. The Justice and Home Affairs Committee report, 'Technology Rules? The advent of new technologies in the justice system' (March 2022), offers many examples - some provided by Public Law Project - such as the Home Office's sham marriage algorithm, which helps determine whether an intended marriage should be investigated as a 'sham' (para. 127). While the use of big data and automated decision-making tools can result in quicker and more consistent outcomes, there is currently a lack of transparency and accountability in how they operate, and existing safeguards under data protection law and elsewhere are not always fully implemented.

2. As a consequence of this opacity and lack of protections, and because such decision-making can have huge consequences on people's lives, these systems carry a very real risk of discrimination and harm. This is the context in which the Data Protection and Digital Information Bill has been introduced. It follows a consultation, 'Data: a new direction', held at the end of 2021. The Government response to the consultation acknowledged widespread support for existing protections and safeguards, such as the requirement to undertake data protection impact assessments and the right not to be subject to solely automated decision-making. Despite this, as currently drafted, the Bill would mean sweeping changes to data protection law, including both the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR) - changes which prioritise economic growth and innovation over rights-protection, transparency and accountability. While the Bill does not outright remove any of the current protections in data protection law it weakens many of them to the extent that they will struggle to achieve their original purposes.
3. This briefing for second reading in the House of Commons identifies a series of issues with the Bill regarding transparency, accountability and the wider context of increased delegated powers, including the deficiency in Parliamentary scrutiny they create. PLP continue to be concerned that many of the proposals set out in the Bill will undermine how effectively people, especially those who are vulnerable or marginalised, can both protect and access their data in future.

   We therefore make the following recommendations:

   - That Members use the second reading to highlight the risks this Bill proposes to data protection provisions and the impact of this for marginalised groups who are often the individuals who are subject to increased scrutiny and decision-making by algorithmic technology.
   - Clause 7 should be removed from the Bill: it significantly limits people's ability to access information about how their personal data is being collected and used.
   - Clause 9 should be removed from the Bill: it curtails the right of the data subject to be informed of how their data is used.
   - Clause 11 is removed and Article 22 - the requirement for human oversight - is retained as a prohibition on solely automated decision-making.

- Changes to Clause 17 that lower the minimum requirements of an impact assessment should be removed from the Bill.

- That Members question why Clauses 5 and 6 of the Bill contain broad and unspecified powers for the Secretary of State to amend the UK GDPR via statutory instrument, without scrutiny by Parliament.

- Clause 106 should be narrowed to allow ministers to make provisions that are consequential on the Act only were necessary, as recommended by the Delegated Powers and Regulatory Reform Committee.

- Clause 11(1) Article 22D(1) of the Bill which allows the Secretary of State to make regulations altering the definition of what is a similarly significant effect of being subject to solely automated decision-making must include a definition of the meaning of a 'similarly significant effect' and the implications it has for individuals.

4. The Bill is long and complex, and it is difficult to understand the changes without a side-by-side comparison with the original text. We have therefore included an Annex in the form of a table with such analysis. By comparing the changes, the Bill proposes alongside how the current law operates, we have identified where we think protections are being weakened. This table is annexed to the end of the Briefing.

Introduction: A data protection shortfall

5. Currently there is insufficient protection, overcollection, and overprocessing of data by government bodies on already marginalized groups - such as those arriving by small boats from France and individuals in the welfare system. This illustrates the importance of data protection in safeguarding rights and the risks of watering them down. Earlier this year the Justice and Home Affairs Committee (JHAC) published its report on new technologies and the application of the law, stressing that without transparency, there is no accountability for when things go wrong. It has been recognised that the surge in data collection, processing, and use of automated systems by government does not affect all communities equally. Professor Karen Yeung highlighted that risk assessment tools are not being developed to "identify insider trading or who is going to commit the next kind of corporate fraud... we are turning it into prediction tools about poor people".

6. The watering down of rights protections proposed by this Bill poses additional risks for marginalised groups, as they are often the individuals who are subject to increased scrutiny and decision-making by algorithmic technology. Without robust data protections, unfair, disproportionate and unlawful practices could leave marginalised individuals exposed to even higher levels of intrusive data collection and processing, exposing them to significant harm.

Parliamentarians may wish to be mindful of these risks as the Bill will weaken data protection provisions.

Clause 7 and 9: Reduced access to personal data and knowledge about how it is used

7. Transparency around government use of big data and automated decision-making tools has intrinsic value; people have a right to know how they are being governed. Transparency has consequential value, too. It facilitates democratic consensus-building about the appropriate use of new technologies, and it is a prerequisite for holding government (and other influential entities) to account when things go wrong.[1] However, clauses 7 and 9 would seriously limit people's ability to access information about how their personal data is being collected and used. This includes limiting access to information about automated decision-making processes to which they are subject.

The problem with Clause 7:

A data subject is someone who can be identified, directly or indirectly, by personal data such as a name, an ID number, location data, or information relating to their physical, economic, cultural or social identity.

Under existing laws, data subjects have a right to request confirmation as to whether their personal data is being processed by a controller, to access that personal data, and to obtain information about how it is being processed as per Article 15 of the UK GDPR. Section 53 of the DPA and Article 12 of the UK GDPR state that a controller can only refuse a request from a data subject if it is 'manifestly unfounded or excessive'.

There are three main ways in which clause 7 significantly limits people's ability to access information about how their personal data is being collected and used:

First, it would lower the threshold to 'vexatious or excessive'. This is an inappropriately low threshold given the nature of a data subject access request, namely, a request by an individual for their own data.

Second, clause 7 would insert a new, mandatory list of considerations for deciding whether a request is vexatious or excessive. This includes vague considerations such as 'the relationship between the person making the request (the "sender") and the person receiving it (the "recipient")'.

Third, the proposed changes to Article 12 and section 53 would mean that they are open to a very wide interpretation and could be relied upon more often by public bodies to refuse data subject access requests - thereby unfairly limiting people's access to their own data.

PLP recommends that this clause be removed from the Bill.

The problem with Clause 9:

Currently, data subjects have a right to be informed about the collection and use of their personal

[1] Public Law Project has conducted comparative and theoretical research on algorithmic transparency. See 'Executable versions: an argument for compulsory disclosure, Part One' (3 August 2022), Digital Constitutionalist, available at https://digi-con.org/executable-versions-part-one/.

data enshrined in Articles 13 and 14 of the UK GDPR. Clause 9 would seriously restrict this right and should be resisted.

Sometimes, a data controller will want to use personal data for additional purposes, other than those for which it was originally collected. Under Article 13(3), a data subject has a right to know about this.
PLP strongly opposes the inclusion of clause 9 in the Bill because it would place new limitations on this right in cases where the additional purposes are for 'scientific or historical research', 'archiving in the public interest' or 'statistical purposes'. These terms are very vague and open to wide interpretation. Scientific research is defined as 'any research that can reasonably be described as scientific, whether publicly or privately funded, including processing for the purposes of technological development or demonstration, fundamental research or applied research'. This could enable private companies carte blanche to use personal data for the purposes of developing new products without needing to inform the data subject.

The effect of such changes to Article 13 are likely to mean that data subjects are less likely to receive information about the processing of their personal data for purposes other than those for which it was collected.

Why clause 9 should be removed from the Bill:

Article 14 provides data subjects with rights to know how their personal data is being processed in cases where the data was not obtained from the data subject themselves. Article 14(5) provides for exemptions – situations where information need not be provided.

Clause 9 would expand this list of exemptions to include situations where 'providing information is impossible or would involve a disproportionate effort' and the obligation to provide information 'is likely to render impossible or seriously impair the achievement of the objectives of the processing'. This would curtail the right of the data subject to be informed and is likely to mean that personal data is processed without the data subject's knowledge in a wider range of situations. Personal data could be used in a range of contexts such as development of credit rating products or in dating apps without the data subject's knowledge.

For these reasons, PLP recommends that clause 9 is removed from the Bill.

Clause 11: Reduced protections against solely automated decision-making

8. Automated decision-making is increasingly used in a range of high-stakes contexts, including immigration, policing, and welfare benefits. The particular risks and problems that arise in relation to solely automated decision-making, are well-accepted. It is not only that human oversight can help to guard against a machine's mistakes and mitigate risks such an encoded bias; there is also a concern about human dignity, and a sense that decisions about human beings should not be made solely on the basis of a data profile.

9. The Government data consultation response acknowledges that, for respondents, 'the right to human review of an automated decision was a key safeguard'. PLP has written about the importance of the prohibition on solely automated decision-making for Prospect magazine: 'Human oversight is crucial for automated decision-making. So why is it being reduced?' (6 December 2021). Despite the

government acknowledging the importance of human review in an automated decision, if implemented, clause 11 would mean that solely automated decision-making is permitted is a wider range of contexts.

The problem with Clause 11:

Currently, Sections 49 and 50 DPA and Article 22 of the UK GDPR provide a right not to be subject to a decision based solely on automated processing, with some narrow exemptions.

Clause 11 introduces a new Article 22B under which solely automated decision-making would be allowed, unless it is a 'significant decision' and it is based on the special categories of personal data referred to in Article 9(1)[2] - in which case, specified conditions must be met. Similarly, the insertion of section 50B would mean that solely automated decision-making is allowed, unless it is a 'significant decision' and it is based on 'sensitive personal data' - in which case, again, one of the conditions must be met. The conditions are that the automated decision-making is required or authorised by law or the data subject has explicitly consented. As part of this change, solely automated decisions that process financial or education data about a person are now permissible.

It is also unclear what will meet the threshold of a 'significant decision'. The Charity Big Brother Watch has identified Local Authorities which use predictive models to identify children deemed at high risk of committing crimes and to include them on a database. Would a decision to include someone on a database meet the threshold of a significant decision?

The impact of clause 11:

These changes would mean that solely automated decision-making is permitted in a much wider range of contexts. It is especially concerning given that many high-impact algorithmic decisions may not involve processing of special categories of personal data.

Further, the proposed changes would mean that Article 22 will no longer be cast as a right not to be subject to solely automated decision-making, but rather as a restriction on solely automated decision-making.

PLP recommends that Article 22 is retained as a prohibition on solely automated decision-making and that clause 11 is removed from the Bill.

Clause 17: Watered-down impact assessments

10. Data Protection Impact Assessments are currently required under Article 35 of the UK GDPR and are essential for ensuring that organisations do not deploy - and individuals are not subjected to - systems that may lead to unlawful, rights-violating or discriminatory outcomes. The Government

[2] The special categories of personal data under Article 9(1) are those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

data consultation response noted that '[t]he majority of respondents agreed that data protection impact assessments requirements are helpful in identifying and mitigating risk and disagreed with the proposal to remove the requirement' to undertake them. However, under clause 17, the requirement to perform an assessment would be seriously diluted.

The problem with Clause 17:

Under clause 17, the minimum requirements of an impact assessment would be lowered. Instead of a systematic description of the processing operations and purposes, the controller would only be required to summarise the purposes of the processing. This would mean that limited consideration is given to how the processing works and the risks this might pose.

Instead of a proportionality assessment, under this provision, the controller would only be required to consider whether the processing is necessary for the stated purposes. Proportionality is the legal test for deciding whether an infringement on human rights (including the right not to be discriminated against) is justified and lawful.

By limiting the requirements of an assessment to include only whether the processing is necessary – not whether it is proportionate – the proposed changes to Article 35 present a serious threat to human rights, and could lead to an increase in discriminatory processing

PLP do not consider these changes necessary or desirable, and they should be removed from the Bill.

Clause 5, 6, 11 and 109: increased delegated powers mean less Parliamentary scrutiny

11. The Bill contains a number of wide delegated powers giving the Secretary of State the power to amend the UK GDPR via statutory instrument. The Government has said that the UK GDPR's key elements remain sound and that it wants to continue to offer a high level of protection for the public's data[3] but this is no guarantee against significant reforms being brought in through a process which eludes parliamentary scrutiny. Proposed changes to the UK GDPR should be on the face of the Bill where they can be debated and scrutinised properly via the primary legislation process. As it stands, key provisions of the UK GDPR are to be subsequently amended via statutory instrument, an inappropriate legislative process that affords much less scrutiny and debate, if debates are held at all.

12. The Government's position is that it is amending the UK GDPR to provide clarity for data processors and for the Information Commissioner in exercising their duties.[4] In fact leaving the UK GDPR open to future amendment via statutory instrument only adds to uncertainty for data processors.

[3] https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation#:~:text=The%20government%20launched%20its%20consultation,the%20UK's%20National%20Data%20Strategy.
[4] See Explanatory Notes to the Bill at [11] and [13].

The problem with these clauses:

Clause 5

The UK GDPR contains a finite set of lawful bases on which personal data can be processed. The protections provided by the UK GDPR currently could be easily undermined if the situations in which a data processor can lawfully process data were too numerous.

Clause 5(4) of the Bill adds a provision allowing personal data to be processed on the basis of a legitimate interest and allows the Secretary of State via statutory instrument to lay regulations defining a legitimate interest.

If there are additional circumstances in which the Government believes the processing of personal data should be permitted, those circumstances should be enumerated on the face of the Bill where they can be subject to debate and scrutiny by Parliament.

Clause 6

Clause 6(5) of the Bill inserts Article 8A which allows the Secretary of State via statutory instrument to add other conditions in which further processing of personal data, beyond the original purpose for which the data was collected, is lawful.

If there are other circumstances in which the Government thinks it should be lawful to further process personal data, those should be contained within the Bill, rather than left to ministers to determine at a later date without scrutiny.

Clause 11

The UK GDPR protects the public from being subject to solely automated decision-making where the decision has legal or 'similarly significant effects'. Clause 11(1) of the Bill inserts Article 22D(1) which allows the Secretary of State to make regulations altering the definition of what is a similarly significant effect. As currently drafted, this provision means ministers can lay regulations narrowing the definition.

For example, the A-level algorithm grading scandal in the summer of 2021, which PLP has written about for the UKCLA: '[Model students: why Ofqual has a legal duty to disclose the details of its model for calculating GCSE and A level grades]' (July 2022). If something like this was to reoccur, a minister could lay regulations stating that the decision to use an algorithm in grading A-levels was not a decision with 'similarly significant effects'.

The meaning of a 'similarly significant effect' should be defined and debated within primary legislation.

Clause 106

Clause 106 of the Bill is a widely drafted Henry VIII power that gives the Secretary of State the power to 'make provision that is consequential on any provision made by this Act'. The Delegated Powers and Regulatory Reform Committee have stated that powers which make consequential provision 'inherently lack a clear definition to its scope' and that consequential changes should 'therefore be restricted by some type of objective test of 'necessity'.[5] In the Bill, what is 'consequential' is left to the subjective judgment of ministers.

We recommend that clause 106 is narrowed to allow ministers to make provisions that are consequential on the Act only were necessary.

Appendix

Clause	Current provision	Proposed change	Commentary

[5] DPRRC (2017–19), 3rd Report, HL Paper 22, paras. 71, 72, 74.

Part 1 Clause 1 Definition of personal data	Sections 3(2) and (3) DPA (2) "Personal data" means any information relating to an identified or identifiable living individual (subject to subsection (14)(c)). (3) "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to— (a) an identifier such as a name, an identification number, location data or an online identifier, or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.	Insert sections 3(3A) and 3(3B) "(3A) An individual is identifiable from information "directly" if the individual can be identified without the use of additional information. (3B) An individual is identifiable from information "indirectly" if the individual can be identified only with the use of additional information." Insert section 3A "Information only relates to an identifiable living individual if – (a) the living individual is identifiable by the controller or processor by reasonable means at the time of the processing; or (b) the controller or processor knows, or ought reasonably to know, that another person will, or is likely to, obtain the information as a result of the processing, and the living individual will be, or is likely to be, identifiable by that person by reasonable means at the time of the processing."	The right to personal data protection is closely connected with the right to respect for private life under Article 8 ECHR (*S and Marper v. the United Kingdom*). Both protect similar values – autonomy and dignity – and offer individuals a protected sphere to think, form opinions and develop their personalities. They are the foundation of other rights, such as freedom of speech, freedom of conscience and religion and the right to protest and assembly. But the ECHR (and UDHR) and the rights contained within them pre-existed the age of the internet. Data protection law, and concepts like 'personal data', were developed specifically in response to new risks posed by computer technology to the right to private life. The insertion of section 3A introduces an explicit reasonableness constraint on the definition of personal data. The new definition is significant, because "personal data" is the touchstone for a number of protections: unless it's personal data, various protections will not apply. Under the new definition, information is not personal data if a controller or processor could not reasonably have identified the individual it relates to at the time of processing (and nor could any third party who was likely to obtain the information).

			In some respects, this does not appear to be a major departure from the current position. According to Recital 26 of the GDPR, the current test is whether it is likely that reasonable means for identification will be available and administered by the foreseeable users of the information; this includes information held by third-party recipients. Further, sections 3(3A) and 3(3B) reflect a distinction already present in EU case law. In *Breyer v. Bundesrepublik Deutschland,* the CJEU dealt with indirect identification and held that "it is not required that all information enabling the identification of the data subject must be held in the hands of one person" for information to constitute personal data. However, it is important to note that section 3A, read with section 3(3B) may narrow the definition of personal data post-*Breyer* because the test in *Breyer* was whether there was a 'more than a hypothetical risk' of third parties obtaining additional information that would allow them to identify an individual. This is wider than 'knew or reasonable ought to know'.

Part 1 Clause 6 Purpose limitation	Article 6 GDPR 1. Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, 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. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks. 2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely	6 The purpose limitation (1) The UK GDPR is amended in accordance with subsections (2) to (5). (2) In Article 5(1)(b) (purpose limitation)— (a) after "collected" insert "(whether from the data subject or otherwise)", (b) after "further processed" insert "by or on behalf of a controller", and (c) for the words "those purposes;" to "initial purposes" substitute "the purposes for which the controller collected the data". (3) In Article 5, at the end insert— "3. For the avoidance of doubt, processing is not lawful by virtue only of being processing in a manner that is compatible with the purposes for which the personal data was collected." (4) In Article 6 (lawfulness of processing), omit paragraph 4. (5) After Article 8 insert— "Article 8A Purpose limitation: further processing 1. This Article is about the determination, for the purposes of Article 5(1)(b) (purpose limitation), of whether processing of personal data by or on behalf of a controller for a purpose (a "new purpose") other than the purpose for	Purpose limitation requires that data is only collected for specific purposes and is not used for purposes or retained for longer than is necessary to achieve those purposes. Annex 2 to the Bill lists purposes for which personal data can be further processed without the data subject's consent if there was an initial lawful basis for processing. It also allows the Secretary of State via secondary legislation to add to that list of lawful purposes. Purposes listed in Annex 2 include processing on the basis of public security, emergencies or the detection or apprehension of crime. No further information about the storage periods and the applicable safeguards for these additional processing purposes are provided within the Annex.

	specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX. 3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by: (a) Union law; or (b) Member State law to which the controller is subject. The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued. 4. Where the processing for a purpose other than that for which the personal data have been	which the controller collected the data ("the original purpose") is processing in a manner compatible with the original purpose. 2. In making the determination, a person must take into account, among other things— (a) any link between the original purpose and the new purpose; (b) the context in which the personal data was collected, including the relationship between the data subject and the controller; (c) the nature of the personal data, including whether it is a special category of personal data (see Article 9) or personal data related to criminal convictions and offences (see Article 10); (d) the possible consequences of the intended processing for data subjects; (e) the existence of appropriate safeguards (for example, encryption or pseudonymisation). 3. Processing of personal data for a new purpose is to be treated as processing in a manner compatible with the original purpose where— (a) the data subject consents to the processing of personal data for the new purpose and the new purpose is specified, explicit and legitimate, (b) the processing is carried out in accordance with Article 84B—(i) for the purposes of scientific research or historical research, (ii) for the purposes of archiving in the public interest, or (iii) for statistical purposes,	

	collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.	(c) the processing is carried out for the purposes of ensuring that processing of personal data complies with Article 5(1) or demonstrating that it does so, (d) the processing meets a condition in Annex 2, or (e) the processing is necessary to safeguard an objective listed in Article 23(1)(c) to (j) and is authorised by an enactment or rule of law. 4. Where the controller collected the personal data based on Article 6(1)(a) (data subject's consent), processing for a new purpose is only processing in a manner compatible with the original purpose if— (a) it falls within paragraph 3(a) or (c), or (b) it falls within paragraph 3(d) or (e) and the controller cannot be reasonably expected to obtain the data subject's consent. 5. The Secretary of State may by regulations amend Annex 2 by— (a) adding or varying provisions, or (b) omitting provisions added by regulations made under this Paragraph. 6. The Secretary of State may only make regulations under paragraph 5 adding a case to Annex 2 where the Secretary of State considers that processing in that case is necessary to safeguard an objective listed in Article 23(1)(c) to (j).	

		7. Regulations under paragraph 5 may make provision identifying processing by any means, including by reference to the controller, the data subject, the personal data or the provision of Article 6(1) relied on for the purposes of the processing. 8. Regulations under paragraph 5 are subject to the affirmative resolution procedure." (6) Schedule 2 inserts Annex 2 to the UK GDPR. (7) The 2018 Act is amended in accordance with subsections (8) to (10). (8) In section 36(1) (the second data protection principle)— (a) in paragraph (a), for "on any occasion" substitute "(whether from the data subject or otherwise)", and (b) in paragraph (b)— (i) after "processed" insert "by or on behalf of a controller", and (ii) for "it was collected" substitute "the controller collected it". (9) In section 87(1) (the second data protection principle)— (a) in paragraph (a), for "on any occasion" substitute "(whether from the data subject or otherwise)", and (b) in paragraph (b)— (i) after "processed" insert "by or on behalf of a controller", and (ii) for "it was collected" substitute "the controller collected it".	

		(10) In Part 1 of Schedule 2 (adaptations and restrictions as described in Articles 6(3) and 23(1)), in paragraph 1, omit sub-paragraph (b)(ii).	
Part 1 Clause 7 Vexatious and excessive requests	Article 12, paragraph 2 GDPR The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject. […]	Insert at the end of paragraph 2 "(or refusal is allowed under Article 12A)" Insert Article 12A Article 12A deals with "vexatious or excessive" requests by data subjects. Where a request from a data subject under any of Articles 15 to 22 or 34 is "vexatious or excessive", the controller may (a) charge a reasonable fee; or (b) refuse to act on the request.	The changes to section 53 would mean that a request can be refused if it is either vexatious or excessive. 'Vexatious' is arguably lower bar than 'manifestly unfounded', under section 53 DPA. It may be an inappropriately low threshold given the nature of a data subject access request - which is a request by an individual for their *own* data. There is a list of examples of a vexatious request under section 204A. This may help to ensure that the provision is not abused.
	Section 53 DPA	In section 53 DPA, "manifestly unfounded" is replaced with "vexatious".	However, the list of examples is non-exhaustive. This means that the term 'vexatious' could

	(1) Where a request from a data subject under section 45, 46, 47 or 50 is manifestly unfounded or excessive, the controller may— (a) charge a reasonable fee for dealing with the request, or (b) refuse to act on the request. (2) An example of a request that may be excessive is one that merely repeats the substance of previous requests. […]		still be taken to include, for example, repeated requests that are considered by the recipient to be without merit. Further, the considerations for determining whether a request is vexatious or excessive are vague. For example, regard must be had to 'the relationship between the person making the request (the "sender") and the person receiving it (the "recipient")'. There is, however, no guidance as to what kind of relationship could potentially mean that a request is vexatious or excessive. Overall, we are concerned that the changes to section 53 would mean that it is open to a very wide interpretation and could be relied upon more often by public bodies to refuse data subject access requests – thereby unfairly limiting people's access to their own data. The Government's Data Consultation document acknowledged that the ability of an individual to access their own data is a fundamental right, and thus we reinstate our argument (para 50 of PLP's response) that measures to limit this right are not acceptable in relation to the rights of data subjects.
	N/a	Insert section 204A Section 204A gives guidance on when a request is vexatious of excessive. "(1) For the purposes of this Act, whether a request is vexatious or excessive must be determined having regard to the circumstances of the request, including (so far as relevant)— (a) the nature of the request, (b) the relationship between the person making the request (the "sender") and the person receiving it (the "recipient"), (c) the resources available to the recipient, (d) the extent to which the request repeats a previous request made by the sender to the recipient, (e) how long ago any previous request was made, and (f) whether the request overlaps with other requests made by the sender to the recipient.	

		(2) For the purposes of this Act, examples of requests that may be vexatious include requests that— (a) are intended to cause distress, (b) are not made in good faith, or (c) are an abuse of process."	
Part 1 Clause 9 (read with Clause 22) **Right to be informed**	Article 13 GDPR 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of relevant adequacy regulations under section 17A of the 2018 Act, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or	Clause 9 would insert at the end of Article 13 GDPR the following: "5. Paragraph 3 does not apply to the extent that— (a) the controller intends to further process the personal data— (i) for (and only for) the purposes of scientific or historical research, the purposes of archiving in the public interest or statistical purposes, and (ii) in accordance with Article 84B, and (b) providing the information is impossible or would involve a disproportionate effort. 6. For the purposes of paragraph 5(b), whether providing information would involve a disproportionate effort depends on, among other things, the number of data subjects, the age of the personal data and any appropriate safeguards applied to the processing." Clause 22 would insert a new Chapter 8A to the UK GDPR, covering 'Safeguards for processing for research, archiving or statistical [RAS] purposes', including:	As it stands, Article 13(3) requires that, if a controller intends to further process personal data, for purposes other than that for which the data was collected, they must inform the data subject and provide the information required under Article 13(2). This includes the purposes and legal basis of the processing, and meaningful information about any automated decision-making conducted using the personal data. The proposed changes to Article 13 would limit the application of this right to be informed. Article 13(3) would no longer apply if the controller intends to further process the personal data for the purposes of scientific or historical research; for purposes of archiving in the public interest; or for statistical purposes *and* the processing is in accordance with Article 84B *and* providing the information is impossible or would involve disproportionate effort. The additional purposes for which personal data can be processed without providing information to the data subject – 'scientific or historical

	suitable safeguards and the means by which to obtain a copy of them or where they have been made available. 2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (d) the right to lodge a complaint with the Commissioner; (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the	"Article 84B - Additional requirements when processing for RAS purposes 1. Processing of personal data for RAS purposes must be carried out subject to appropriate safeguards for the rights and freedoms of the data subject. 2. Processing of personal data for RAS purposes must be carried out in a manner which does not permit the identification of a living individual. 3. Paragraph 2 does not apply— (a) to the collection of personal data (whether from the data subject or otherwise), or (b) to cases in which the RAS purposes cannot be fulfilled by further processing in the manner described in that paragraph. 4. For the purposes of paragraph 2, processing permits the identification of a living individual only in cases described in section 3A(2) and (3) of the 2018 Act (information relating to an identifiable living individual). Article 84C - Appropriate safeguards 1. This Article makes provision about when the requirement under Article 84B(1) for processing to be carried out subject to appropriate safeguards is satisfied.	research', 'archiving in the public interest' or 'statistical purposes' - are phrased in vague terms and are open to very wide interpretation. Further, Article 84B merely requires that processing for research, archiving or statistical (RAS) purposes is carried out subject to 'appropriate safeguards'. This term is not defined and examples of appropriate safeguards are not listed. Article 84C gives some limited guidance on when the appropriate safeguards requirement is met. However, Article 84C is vague and far from comprehensive and is not sufficient to ensure that adequate safeguards being put in place. Overall, the changes to Article 13 are likely to mean that data subjects are less likely to receive information about the processing of their personal data for purposes other than those for which it was collected.

	significance and the envisaged consequences of such processing for the data subject. 3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. 4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.	2. The requirement is not satisfied if the processing is likely to cause substantial damage or substantial distress to a data subject. 3. The requirement is not satisfied if the processing is carried out for the purposes of measures or decisions with respect to a particular data subject, except where the purposes for which the processing is carried out include the purposes of approved medical research. 4. The requirement is only satisfied if the safeguards include technical and organisational measures for the purpose of ensuring respect for the principle of data minimisation (see Article 5(1)(c)), such as, for example, pseudonymisation. […]"	
	Article 14 GDPR 1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) the categories of personal data concerned;	The following changes are to be made to Article 14: "(a) in paragraph 5— (i) for "shall not apply where and insofar as" substitute "do not apply to the extent that", (ii) omit point (b), (iii) omit "or" at the end of point (c), (iv) in point (d), omit "where", and (v) after that point insert— "(e) providing the information is impossible or would involve a disproportionate effort, or (f) the obligation referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of the processing for	As it stands, Article 14 provides data subjects with rights to know how their personal data is being processed when the data was not obtained from the data subject. Article 14(5) provides for exemptions – situations where information need not be provided. The proposed changes would expand this list of exemptions to include situations where 'providing information is impossible or would involve a disproportionate effort' and the obligation to provide information 'is likely to render

	(e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of relevant adequacy regulations under section 17A of the 2018 Act, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available. 2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability; (d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;	which the personal data are intended." (b) at the end insert— "6. For the purposes of paragraph 5(e), whether providing information would involve a disproportionate effort depends on, among other things, the number of data subjects, the age of the personal data and any appropriate safeguards applied to the processing. 7. A controller relying on paragraph 5(e) or (f) must take appropriate measures to protect the data subject's rights, freedoms and legitimate interests, including by making the information available publicly."""	impossible or seriously impair the achievement of the objectives of the processing'. This is concerning, because it curtails the right to be informed and will mean that personal data is processed without data subject's knowledge in a wider range of situations.

	(e) the right to lodge a complaint with the Commissioner; (f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources; (g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. 3. The controller shall provide the information referred to in paragraphs 1 and 2: (a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed. 4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. 5. Paragraphs 1 to 4 shall not apply where and insofar as:		

	(a) the data subject already has the information; (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available; (c) obtaining or disclosure is expressly laid down a provision of domestic law which provides appropriate measures to protect the data subject's legitimate interests; or (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by domestic law, including a statutory obligation of secrecy.		
Part 1 Clause 11 Protection against solely automated decision-making	Article 22 GDPR 1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. 2. Paragraph 1 shall not apply if the decision:	Substitute Article 22 with Articles 22A-22D Article 22A defines key terms. (1)(a) a decision is based solely on automated processing if there is no meaningful human involvement in the taking of the decision. (1)(b) a decision is a significant decision, in relation to a data subject, if—	To an extent, Article 22A(1)(a) offers some useful clarity. It specifies that, unless there is meaningful human involvement in the taking of the decision, it is a decision based solely on automated processing. Whether there is meaningful human involvement may, however, be difficult to determine in practice, not least because of the problem of

	a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or c) is based on the data subject's explicit consent. 3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. 4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place. […]	(i) it produces a legal effect for the data subject, or (ii) it has a similarly significant effect for the data subject. (2) References in this Article and Articles 22B to 22D to a decision and to taking a decision include profiling and carrying out profiling.	automation bias. As articulated in paras 21-25 of our response to the Data Consultation, human oversight or involvement under a broad interpretation of Article 22 can effectively be a token gesture or amount to 'rubber-stamping'. The definition of a 'significant' decision under Article 22A(1)(b) reflects the existing touchstone under Article 22: "legal or similarly significant effect". In our article for Prospect, we argued that Article 22 as currently drafted is not perfect and there is a strong case for reform—but to make oversight stronger, not weaker. The problem remains that the safeguard against solely automated decision-making is open to a very narrow interpretation, under which many if not most ADM systems would be excluded from its scope.
		Article 22B places some restrictions on solely automated decision-making. "1. A significant decision based entirely or partly on special categories of personal data referred to in Article 9(1) may not be taken based solely on automated processing, unless one of the following conditions is met. 2. The first condition is that the decision is based entirely on processing of personal data to which the data subject has given explicit consent.	The European Union Agency for Fundamental Rights Handbook on European Data Protection Law summarises the effect of Article 22 as follows: "According to the Article 29 Working Party, the right not to be subject to decisions based solely on automated processing that may result in legal effects for the data subject or that significantly affect him or her equates to a general prohibition and does not require the data subject to proactively seek an objection to such a decision.

		3. The second condition is that— (a) the decision is— (i) necessary for entering into, or performing, a contract between the data subject and a controller, or (ii) required or authorised by law, and (b) point (g) of Article 9(2) applies.[1] 4. A significant decision may not be taken based solely on automated processing if the processing of personal data carried out by, or on behalf of, the decision-maker for the purposes of the decision is carried out entirely or partly in reliance on Article 6(1)(ea)."	Nevertheless, according to the GDPR, automated decision-making with legal effects or that significantly affect individuals may be acceptable if it is necessary for entering a contract or the performance of a contract between the data controller and data subject, or if the data subject gave explicit consent. Also, automated decision-making is acceptable if it is authorised by law and if the data subject's rights, freedoms and legitimate interests are appropriately safeguarded." Under Article 22B, solely automated decision-making is allowed, unless it is a 'significant decision' *and* it is based on special categories of personal data referred to in Article 9(1) - in which case, one of the conditions must be met. The special categories of personal data under Article 9(1) are those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. This new stipulation is concerning, because many of the high stakes algorithmic decisions we are concerned about may not involve

			processing of these special categories of personal data. Further, the proposed changes would mean that, in the UK, Article 22 is longer be cast as a right, but rather as a restriction on solely automated decision-making. Note that the drafting of the second condition seems odd - presumably, the intended effect is that decisions based on ethnicity, sexuality, etc require a legal basis. However, the condition is phrased in such a way that solely automated decision-making is only allowed if it's a decision based on ethnicity etc *and* there is a legal basis. What if it's not a decision based on ethnicity etc, but there is a legal basis? Why should a basis in protected characteristics be a *condition* of solely automated processing? This point aside, the circumstances in which solely automated decision-making is permitted seem substantially similar to those that already exist under Article 22.
		Article 22C requires safeguards to be put in place in relation to solely automated decision-making. "1. Where a significant decision taken by or on behalf of a controller is— (a) based entirely or partly on personal data, and	Under Article 22(3), the safeguards must include a right for data subject to obtain human intervention on the part of the controller, to express his or her point of view, and to contest the decision. The safeguards under Article 22C are substantially similar - see, however, section 50C (below) which provides for exemptions from safeguards.

		(b) based solely on automated processing, the controller must ensure that safeguards for the data subject's rights, freedoms and legitimate interests are in place which comply with paragraph 2 and any regulations under Article 22D(3). 2. The safeguards must consist of or include measures which— (a) provide the data subject with information about decisions described in paragraph 1 taken in relation to the data subject; (b) enable the data subject to make representations about such decisions; (c) enable the data subject to obtain human intervention on the part of the controller in relation to such decisions; (d) enable the data subject to contest such decisions."	
	Sections 49 and 50 DPA Section 49: Right not to be subject to automated decision-making (1) A controller may not take a significant decision based solely on automated processing unless that decision is required or authorised by law. (2) A decision is a "significant decision" for the purpose of this section if, in relation to a data subject, it—	Substitute sections 49 and 50 with sections 50A-50C Section 50A "(1) For the purposes of sections 50B and 50C— (a) a decision is based solely on automated processing if there is no meaningful human involvement in the taking of the decision, and (b) a decision is a significant decision, in relation to a data subject, if —	Section 50A departs from the proposed Article 22A and from the current section 49 DPA, in that 'significant decisions' are only those that have an *adverse* effect on the data subject. The rationale for this divergence is unclear, and it is likely to produce unwelcome tension and complexity. The tension should be resolved in favour of the definition under Article 22A. The section 50A definition is too limited, and may be unworkable in

	(a) produces an adverse legal effect concerning the data subject, or (b) significantly affects the data subject. Section 50: Automated decision-making authorised by law: safeguards (1) A decision is a "qualifying significant decision" for the purposes of this section if— (a) it is a significant decision in relation to a data subject, and	(i) it produces an adverse legal effect for the data subject, or (ii) it has a similarly significant adverse effect for the data subject. (2) References in this section and sections 50B to 50D to a decision and to taking a decision include profiling and carrying out profiling."	practice. This is because an automated decision-making system could produce an adverse effect in respect of some individuals but not others. For example, an automated tool used to decide visa applications will have a significant effect in respect of all applicants, but will only have a significant *adverse* effect in respect of some applicants (those whose applications are refused). And yet, safeguards will need to be implemented at a system-level.
	(b) it is required or authorised by law. (2) Where a controller takes a qualifying significant decision in relation to a data subject based solely on automated processing— (a) the controller must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing, and (b) the data subject may, before the end of the period of 1 month beginning with receipt of the notification, request the controller to— (i) reconsider the decision, or (ii)take a new decision that is not based solely on automated processing. (3) If a request is made to a controller under subsection (2), the controller must, before the end of	Section 50B places restrictions on solely automated decision-making "(1) A significant decision based entirely or partly on sensitive personal data may not be taken based solely on automated processing, unless one of the following conditions is met. (2) The first condition is that the decision is based entirely on processing of personal data to which the data subject has given explicit consent. (3) The second condition is that the decision is required or authorised by law."	The insertion of section 50B would mean that solely automated decision-making is allowed, unless it is a 'significant decision' *and* it is based on 'sensitive personal data' - in which case, one of the conditions must be met. The conditions are that it's required or authorised by law or the data subject has explicitly consented. The 'sensitive personal data' stipulation is new, and means that solely automated decision-making is permitted in a wider range of contexts. 'Sensitive personal data' is not defined, but is likely intended to refer to the special categories of personal data under Article 9. As above (Article 22B), this new stipulation is concerning, because many of the high stakes algorithmic decisions we are concerned about may not involve processing of sensitive personal data.

	the period of 1 month beginning with receipt of the request— (a) consider the request, including any information provided by the data subject that is relevant to it, (b) comply with the request, and (c)by notice in writing inform the data subject of— (i) the steps taken to comply with the request, and (ii) the outcome of complying with the request. [...]		
		Section 50C provides for safeguards and exemptions to safeguards. (1) Subject to subsection (3), where a significant decision taken by or on behalf of a controller is— (a) based entirely or partly on personal data, and (b) based solely on automated processing, the controller must ensure that safeguards for the data subject's rights, freedoms and legitimate interests are in place which comply with subsection (2) and any regulations under section 50D(3). (2) The safeguards must consist of or include measures which— (a) provide the data subject with information about decisions described in subsection (1) taken in relation to the data subject; (b) enable the data subject to make representations about such decisions; (c) enable the data subject to obtain human intervention on the part of the controller in relation to such decisions; (d) enable the data subject to contest such decisions. (3) Subsections (1) and (2) do not apply in relation to a significant decision	Section 50C mirrors the safeguards in Article 22C but adds exemptions from the safeguards, listed at section 50C(4). The safeguards apply to solely *and* partly automated decision-making, which is an improvement. However, it is not clear that the 'right to know' would be as robust under section 50C as it currently is under section 50. Under section 50C, the safeguards must include measures which provide the data subject with information about solely or partly automated decisions. But this seems weaker than the requirement under section 50, that a controller must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing. The drafting here is a bit messy, but the effect of subsections 1 and 3 appears to be that safeguards are *always* required in respect of solely automated decision-making, but are *not* always required in respect of partly automated decision-making - if an exemption applies. The exemptions to safeguards mean that the distinction between solely and partly automated decision-making is very significant.

		if— (a) exemption from those provisions is required for a reason listed in subsection (4), and (b) the controller reconsiders the decision, as soon as reasonably practicable, in a manner that is not based solely on automated processing. (4) Those reasons are— (a) to avoid obstructing an official or legal inquiry, investigation or procedure; (b) to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) to protect public security; (d) to safeguard national security; (e) to protect the rights and freedoms of others.	The exemptions may place serious limitations on an individual's right to know that automation is being used, and to make representations, obtain human intervention and contest decisions. Who decides if an exemption is required? Is it the user of the automated tool? If so, their decision should be checked by an independent regulator. We should consider the relationship between these exemptions, FOIA, and any future compulsory transparency regime. Presumably exemptions to compulsory transparency would need to mirror these, to avoid inconsistency? Note that under the Bill, there would be a number of significant differences between the GDPR and the DPA where, currently, they mirror one another. In light of these differences, it will be important to consider the relationship between the two, going forward.
Part 1, Clause 16 Logging of law enforcement processing	Section 62 DPA (1) A controller (or, where personal data is processed on behalf of the controller by a processor, the processor) must keep logs for at least the following processing operations in automated processing systems— (a)collection; (b)alteration; (c)consultation; (d)disclosure (including transfers);	Omit the requirement to provide a justification for consulting data records.	The changes to section 62 would mean that the police are no longer required to log their justification for accessing specific data records. This is a threat to individual rights and allows the police to provide a retrospective justification.

	(e)combination; (f)erasure. (2) The logs of consultation must make it possible to establish— (a)the justification for, and date and time of, the consultation, and (b)so far as possible, the identity of the person who consulted the data. (3) The logs of disclosure must make it possible to establish— (a)the justification for, and date and time of, the disclosure, and (b)so far as possible— (i)the identity of the person who disclosed the data, and (ii)the identity of the recipients of the data. (4) The logs kept under subsection (1) may be used only for one or more of the following purposes— (a)to verify the lawfulness of processing; (b)to assist with self-monitoring by the controller or (as the case may be) the processor, including the conduct of internal disciplinary proceedings; (c)to ensure the integrity and security of personal data; (d)the purposes of criminal proceedings. (5) The controller or (as the case may be) the processor must make the logs available to the Commissioner on request.		
Part 1 Clause 17 Assessments of High Risk Processing	Article 35 GDPR 1. 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	Substitute Article 35(7) with the following: "The controller must produce a document recording compliance with this Article which includes at least—	Data Protection Impact Assessments are essential for ensuring that organisations do not deploy - and individuals are not subjected to - systems that may lead to unlawful or discriminatory outcomes.

	high risk to the rights and freedoms of natural persons, 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. […] 7. The assessment shall contain at least: a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	(a) a summary of the purposes of the processing, (b) an assessment of whether the processing is necessary for those purposes, (c) an assessment of the risks to individuals referred to in paragraph 1, and (d) a description of how the controller proposes to mitigate those risks."	Unfortunately, however, they have been framed by government as menial tick-box exercises that place unnecessary administrative burden on data processors. Under these new provisions, the minimum requirements of an assessment would be lowered. Instead of a systematic description of the processing operations and purposes, the controller would only be required to summarise the purposes of the processing. Instead of a proportionality assessment, the controller would only be required to consider whether the processing is necessary for the stated purposes. As expressed in paras 32-37 of our response to the Data Consultation, Data Protection Impact Assessments are an important tool for guarding against some of the risks posed by ADM systems, and thus tis proposal presents a major risk to human rights and could lead to an increase in discriminatory processing. Under the *Bank Mellat* proportionality test, four questions must be considered to decide whether a measure which infringes human rights (including Article 14 ECHR, which guards against discrimination) is justified: (1) whether the objective of the measure is sufficiently important to justify the limitation of a protected right;

			(2) whether the measure is rationally connected to the objective; (3) whether a less intrusive measure could have been used without unacceptably compromising the achievement of the objective; and (4) whether, balancing the severity of the measure's effects on the rights of the persons to whom it applies against the importance of the objective, to the extent that the measure will contribute to its achievement, the former outweighs the latter. By limiting the requirements of an assessment to include only whether the processing is necessary – not whether it is proportionate (as per the four questions above) – the changes to Article 35 make it more likely that people will be subject to processing which is not justified and which violates their human rights.
Part 1 Clause 18 Consultation of the Commissioner prior to high risk processing	Article 36 GDPR 1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.	In paragraph 1 of Article 36 — (a) for "shall" substitute "may", and (b) for "a data protection impact assessment" substitute "an assessment".	The changes to Article 36 would mean that a controller is no longer required to consult the Commissioner prior to carrying out high risk processing ('shall' is substituted for 'may'). Note, however, that this provision is rarely used in practice.
Part 1, Clause 44 Regulations made by Secretary of State	N/a	Insert Article 91A - Regulations made by Secretary of State 1. This Article makes provision about regulations made by the Secretary of State under this Regulation ("UK GDPR	The Bill contains a number of wide delegated powers giving the Secretary of State the power to amend the GDPR via statutory instrument. The Government has said that the GDPR's key elements remain sound and that it wants to

		regulations"). 2. Before making UK GDPR regulations, the Secretary of State must consult— (a) the Commissioner, and (b) such other persons as the Secretary of State considers appropriate. 3. Paragraph 2 does not apply to regulations made under Article 49A where the Secretary of State has made an urgency statement in respect of them. 4. UK GDPR regulations may— (a) make different provision for different purposes; (b) include consequential, supplementary, incidental, transitional, transitory or saving provision. 5. UK GDPR regulations are to be made by statutory instrument. 6. For the purposes of this Regulation, where regulations are subject to "the negative resolution procedure", the statutory instrument containing the regulations is subject to annulment in pursuance of a resolution of either House of Parliament. 7. For the purposes of this Regulation, where regulations are subject to "the affirmative resolution procedure", the regulations may not be made unless a draft of the statutory instrument containing them has been laid before Parliament and approved by a resolution of each House of Parliament.	continue to offer a high level of protection for the public's data.[1] Therefore, it is only right that any proposed changes to the GDPR be contained on the face of the Bill where they can be debated and scrutinised properly via the primary legislation process. It is inappropriate for key provisions of the GDPR to be subsequently amended via statutory instrument, a legislative process that affords much less scrutiny and debate, if debates are held at all. The Government has said that it is amending the UK GDPR in order to provide clarity for data processors and for the Information Commissioner in exercising their duties.[2] In fact leaving the GDPR open to future amendment via statutory instrument only adds to uncertainty for data processors. Furthermore, as mentioned above, it will be important to consider the relationship between the GDPR and DPA - where there are differences between the two, does the DPA supersede the GDPR? Will the GDPR have the status of retained EU law or not, the Bill does not say. If so, how does this affect the significance of the SoS powers to change the GDPR?

		8. For the purposes of this Regulation, where regulations are subject to "the made affirmative resolution procedure"— (a) the statutory instrument containing the regulations must be laid before Parliament after being made, together with the urgency statement in respect of them, and (b) the regulations cease to have effect at the end of the period of 120 days beginning with the day on which the instrument is made, unless within that period the instrument is approved by a resolution of each House of Parliament. 9. In calculating the period of 120 days, no account is to be taken of any whole days that fall within a period during which— (a) Parliament is dissolved or prorogued, or (b) both Houses of Parliament are adjourned for more than 4 days. 10. Where regulations cease to have effect as a result of paragraph 8, that does not— (a) affect anything previously done under the regulations, or (b) prevent the making of new regulations. 11. Any provision that may be included in UK GDPR regulations subject to the negative resolution procedure may be made by regulations subject to the affirmative resolution procedure or the made affirmative resolution	

		procedure. 12. A requirement under this Article to consult may be satisfied by consultation before, as well as by consultation after, the provision conferring the power to make regulations comes into force. 13. In this Article, "urgency statement", in relation to regulations, means a reasoned statement that the Secretary of State considers it desirable for the regulations to come into force without delay."	

Contact

Saba Shakil
Research Fellow
a.sinclair@publiclawproject.org.uk

Mia Leslie
Research Assistant
m.leslie@publiclawproject.org.uk

Anna Sereni
Policy and Parliamentary Officer
a.sereni@publiclawproject.org.uk

Public Law Project is an independent national legal charity.

We are researchers, lawyers, trainers, and public law policy experts.

Our aim is to make sure state decision-making is fair and lawful and that anyone can hold the state to account.

For over 30 years we have represented and supported people marginalised through poverty, discrimination, or disadvantage when they have been affected by unlawful state decision-making.

Public Law Project contributes and responds to consultations, policy proposals, and legislation to ensure public law remedies, access to justice, and the rule of law are not undermined.

We provide evidence to inquiries, reviews, statutory bodies, and parliamentary committees in relation to our areas of expertise, and we publish independent research and guides to increase understanding of public law.

Public Law Project's research and publications are available at:

www.publiclawproject.org.uk/resources-search/