Which?

Written Evidence submitted by Which?

Data Protection & Digital Information (No.2) Bill

Committee Stage (House of Commons)

1. Which? is the UK's consumer champion, here to make life simpler, fairer and safer for everyone. Our research gets to the heart of consumer issues, our advice is impartial, and our rigorous product tests lead to expert recommendations. We're the independent consumer voice that works with politicians and lawmakers, investigates, holds businesses to account and makes change happen. As an organisation we're not for profit and all for making consumers more powerful.

2. The Data Protection & Digital Information (DPDI) Bill will refresh and update the UK's data protection framework. Which? welcomes the opportunity to submit evidence to the Public Bill Committee to highlight how provisions in the Bill can better protect the rights of consumers while supporting greater innovation in our economy.

3. The stated intention of the Bill is to reduce administrative burdens on businesses and encourage growth and innovation in the UK economy. The Bill will also empower consumers through the introduction of a new Smart Data regime, which has the potential to lower prices and improve services as highlighted by Minister Julia Lopez MP at the Bill's Second Reading debate in the House of Commons. The Bill also affirms important safeguards to use data to prevent crime, including fraud.

4. Whilst recognising the value of some of these reforms, Which? is concerned that the current drafting of the legislation may not best serve the rights and interests of consumers. The government should consider reasonable amendments to some of the main provisions to give consumers more confidence and security that their data is safeguarded.

5. We have identified key areas where meaningful changes are needed to ensure consumers are protected from harm:

    - **Automated Decision Making**
      Safeguards for consumers must be more detailed and Secretary of State powers must be accompanied by wide public consultation.

    - **Data-sharing for fraud prevention**
      The Information Commissioner's Office (ICO) must introduce a Code of Practice on data-sharing for the prevention of economic crime, in order to reduce fraud.

    - **Duty to Keep Records**
      The removal of the duty to keep records must only apply to small businesses to protect consumers in the event of a data breach.

    - **Legitimate Interests/Lawfulness of Processing**
      The newly recognised list of legitimate interests must not be expanded to include commercial interests which do not benefit consumers.

- **Subject Access Requests (SARS)**
  Consumers must not be unfairly treated when requesting to access their personal data.

- We also have a number of other concerns about the Bill: the omission of a **collective redress** mechanism; the changes to the **definition of personal data**; and the inclusion of a new list of **further processing** purposes.

Which?'s Principal Concerns

Automated Decision Making

6. Automated decision making **(Part 1, Clause 11)** can bring benefits to consumers by tailoring products and services to better reflect their interests. The use of artificial intelligence (AI) has vastly expanded the range and application of data in such processes, making it ever more complex for consumers to understand. Evidence suggests that consumers feel uncomfortable with automated decision making, particularly when it comes to decisions with high consequences, such as financial ones. An example of this would be if a person's mortgage application could be denied by a credit scoring algorithm even though all the documentation is correct and the person would meet the requirements if it was supervised by an underwriter.

7. Currently, under Article 22 of UK General Data Protections Regulations (UK GDPR), organisations cannot make decisions based solely on automated processing if the decision produces legal effects or significantly affects the data subject. The exceptions are when the decision is necessary for the purposes of a contract between the data subject and an organisation, where the data subject has given explicit consent, or where such decisions are authorised under domestic law. For the latter, section 14 of the Data Protection Act 2018 sets out detailed safeguards to be implemented e.g. the data subject must be given information about the processing, they are able to request that the decision be reconsidered and they can request a new decision not based solely on automated processing.

8. Which? is concerned that the Bill mostly removes the current automated decision making protections for consumers under Article 22 of the GDPR. This states that organisations cannot make decisions based solely on automated processing, except for cases where the explicit exemptions apply, if the decision produces legal effects or similarly significantly affects the data subject. The Bill mostly removes this 'general prohibition'. Given this, detailed safeguards for consumers must be in place to ensure transparency and their right to challenge automated decisions. The safeguards proposed in the Bill at present are not prescriptive enough. Which? recommends remedying this by amending the provision to make clearer the protections and safeguards consumers will have when decisions are made by automated means.[1]

9. The Bill also proposes to give the Secretary of State (SoS) the power to stipulate types of decisions that are, or are not, considered 'significant' and the power to determine when 'meaningful human involvement' has taken place. This is a risk for consumers because restrictions and safeguards in the legislation would not apply to decisions considered not 'significant' or to have had 'meaningful human involvement', which is difficult to define. In addition, it grants the SoS the ability to vary safeguards, such as

[1] N.b The safeguards currently outlined in the new Art 22C of the draft Bill are significantly less detailed / prescriptive than those outlined in section 14 of the UK Data Protection Act 2018.

the right to contest decisions, in the future.

10. This could mean decisions relating to life or health insurance, which are not considered essential financial products, could be classed as not 'significant.' In this case the consumer would lose the protection and right to human review or to present other documentation. Our research shows that consumers feel that the removal of this right would be "dehumanising".

11. To protect the rights of consumers, the ability of the Secretary of State to specify types of decisions which are not to be treated as 'significant' and to vary the safeguards in the future must be removed. The government must also commit in the Bill to wide public consultation on the SoS powers to define 'meaningful human involvement'.

Data sharing for fraud prevention

12. We are pleased that the new list of recognised legitimate interests **(Part 1, Clause 5)** includes the "prevention of crime". This will help facilitate data sharing for the purposes of fraud prevention by removing the obligation for businesses to conduct a balancing test for this processing purpose, where certain criteria are met. We concurrently welcome the publishing of the Governments Fraud Strategy, which includes a number of data-focused solutions to tackling this crime.

13. Cross-sector data sharing of suspicious fraudulent activity has proven to be effective in the prevention of fraud. The activity is not currently widespread, mainly due to concerns from industry around breaching data protection law. The UK is in the midst of a fraud epidemic, with fraud accounting for over 40% of crime. It is critical that businesses make use of this new provision.

14. Which?'s industry engagement has highlighted that businesses find the current ICO guidance unclear and insufficient to encourage them to share data for fraud prevention, particularly data on suspicious activity. To complement the Government's new Fraud Strategy, a new provision could be added to the Bill which mandates the ICO to develop a robust and clear Code of Practice to support businesses to share data to better identify fraudsters and prevent fraud from reaching consumers.

Duty to Keep Records

15. Record keeping is the foundation of many privacy processes. This includes fulfilling requests for access (SARs) and erasure, responding to data breaches, understanding what data an organisation processes and where it is held. This is of great relevance when weighed against the volume of cyber attacks faced by organisations on a daily basis, with 39% of UK businesses having identified a cyber attack in the last 12 months.

16. The removal of the duty to keep records **(Part 1, Clause 15)** on any size business, except in 'high risk' circumstances, will greatly reduce transparency and oversight of consumers' data. It will provide no benefit to large businesses operating across multiple jurisdictions, due to the requirement to keep records under EU GDPR.

17. For many organisations, their record of processing activities is the only way of confidently knowing where data is stored. Take the example of a major cyber attack resulting in a data breach. If there are no formal records then it would be very difficult for the organisation to: check exactly what data was at risk; fully remediate the breach, and; notify all impacted individuals. Consumers may be left unaware of what data was accessed or what appropriate measures they need to take to protect themselves.

18. Only requiring record keeping where processing is 'high risk', which is yet to be defined, is shortsighted. Enforcement action taken by the ICO against organisations who misuse

personal data does not always involve processing that is usually considered as high risk. Such records help an organisation to demonstrate compliance, assess and mitigate risks, and be held to account.

19. We recommend reverting the current duty to keep records proposal back to version 1 of the Bill, removing the duty to keep records for businesses with under 250 employees except where processing is "high risk". This will reduce the burden of record keeping on small businesses, thereby increasing innovation, while ensuring consumers are protected by companies that are likely to hold a large amount of data.

Legitimate Interests/Lawfulness of Processing

20. Which? is not supportive of the ability for the SoS to expand the list of 'recognised legitimate interests' without prior public consultation **(Part 1, Clause 5)**. If a controller has a legitimate interest which is included on the list, the new provisions will enable controllers to prioritise their interests in processing data over the impact on data subjects, by not requiring them to conduct a balancing test. This will result in weaker protections for the data subject. The balancing test is an important safeguard for consumers - removing this for commercial purposes (if the list of recognised legitimate interest was expanded to include these) would lead to a significant reduction of consumer control. Our research demonstrates that consumers understand and value control over how their data is collected and used.

21. It is reasonable to assume that there will be a significant push from companies to push for more 'commercial' interests, such as ad targeting, to be added to the list of 'recognised legitimate interests'. We note the challenge to TiKTok by the Irish and Italian data protection authorities where they were planning to move from a 'consent' basis for targeted ads to a 'legitimate interest'.

22. The Bill should limit additions to this list to those that have a public interest basis, as set out in the objectives listed in Article 23. The Government should also commit to holding a public consultation to allow for proper scrutiny of 'recognised legitimate interest' secondary regulations. Paragraph 1 in Annex 1 of the Bill which sets out the disclosure for processing purposes should be deleted as it is overly broad and does not set out a specific public interest.

Subject Access Requests (SARs)

23. A SAR is a request made by or on behalf of an individual for a record of their personal information held by an organisation. They are an essential tool for consumers' rights and control of their data. This Bill will change the threshold for a data controller to refuse a SAR from the current "manifestly unfounded or excessive" to "vexatious or excessive" **(Part 1, clause 7)**. We do not support this change, as it arguably opens up a broader range of circumstances in which controllers can charge for or refuse requests.

24. This threshold should be better worded to ensure consumer rights and protections are not diminished. For example, the Bill currently suggests that repeat requests may be an indicator of a request being vexatious. However, the Bill does not include reference to whether or not previous requests were complied with as a consideration. This could allow organisations to label new requests 'vexatious' despite their own previous non-compliance.

25. The Bill includes an example of requests that may be vexatious as those that 'are not made in good faith'. This is too subjective and could be open to abuse by the data controller. Increasing the grounds for refusal will exacerbate a sense of powerlessness amongst consumers and could impact on their ability to seek redress. The Government

could strengthen this section through amendments to the definition of vexatious requests to include those that 'have no reasonable foundation'.

26. The Bill should also be amended to add a requirement for controllers to provide evidence of the data subject's vexatious or excessive intention and remove a controller's right to factor in their resources when deciding whether a request is vexatious or excessive. This will better ensure that consumers rights are protected under the new legislation.

Which?'s Other Concerns

Collective Redress and Enforcement

27. The Bill provided an excellent opportunity to implement a collective redress mechanism under **Article 80(2) UK GDPR**. The lack of its inclusion is a disappointment. It severely restricts the ability of organisations like Which? to raise data breach complaints on behalf of the consumers we represent - preventing an important route for the continued protection of consumers and effective enforcement of the law.

28. Which? strongly believes that an effective domestic data protection redress framework requires a **collective redress mechanism** on an opt-out basis to be introduced for violations of data protection law, including significant data breaches. This would help create an environment where data subjects have confidence in the way that organisations are using their data and are assured that there are processes in place to protect their data rights if something goes wrong, domestically or internationally. A collective redress mechanism should be introduced to the text of the Bill.

29. Many companies, particularly larger ones, that are controllers and processors of the data of UK consumers are not based in the UK. For this reason, **Article 27 of the UK GDPR** requires that such companies appoint a UK-based representative to assist consumers and others in communicating with them and helping to ensure that data protection law is observed and enforced. The Bill proposes the deletion of this provision without any clear justification for doing so. We urge that it is maintained. Other provisions in the Bill such as those for 'senior responsible individuals' are not an adequate substitute, and do not require such a person to be located in the UK for the purposes of facilitating service of proceedings or other enforcement matters.

30. We recommend amending the Bill to retain the requirement for non-UK based data controllers to have UK based representatives, and to require the ICO to produce a Code of Practice on the roles and responsibilities of representatives.

Definition of personal data

31. We do not support **Part 1 Clause 1** of the Bill, which will amend the definition of 'personal data'. This will potentially reduce the scope of what is considered 'personal data', by narrowing the consideration of who could identify a person from the data and the time window when the identification could take place.

32. For example, currently a controller or processor has to consider whether anyone could identify the data subject, including at any time in the future, unless data is irreversibly anonymised. Under the new definition, the controller would only have to consider identifiability by the controller or processor and people who are likely to receive the information, and identifiability only at the time of the processing, which appears not to include a continuous obligation. As a result, some data which might currently be classified as 'personal data' (and is therefore subject to the GDPR/DPA regime) may not be classified as such under the new definition, widening situations in which data

protections do not apply.

33. We believe that the definition's reference to 'another person' who is 'likely to' obtain the information means that a controller or processor would not sufficiently have to take into account complex real life situations. This could include how a determined stalker or someone seeking to institute a 'smear' campaign could have a motive and resources to find and use the data in the future - because that may not be deemed 'likely'.

34. Data derived from a consumer using an online service which records location, gender and time could plausibly be used to identify that consumer with some additional cross-referencing by a determined investigator against public records. Under the new definition, businesses may not be obligated to protect the privacy and security of that data as 'personal data' in the same way as under the current law.

35. Similarly, under the current law a controller or processor needs to keep the categorisation of data it holds under careful review to take into account technological developments such as sophisticated new artificial intelligence or 'web-scraping' tools. This would no longer be the case if the Bill is passed in its current form. The Bill therefore should be amended to prevent the government from limiting the definition of personal data to only where an individual is identifiable at the time of the processing. The scope of 'who' the controller has to consider should also be broadened, when considering who might be able to identify a data subject. We would also suggest additional factors for controllers to take into account when considering whether a person is likely to use a means of identifying a data subject, and the addition of an assumption that, if there is doubt as to whether data is 'personal data', then it should be treated as though it is.

Purpose Limitation/Further Processing

36. Under the current regime, the purpose limitation provision (**Article 5(1)(b) UK GDPR**) requires that personal data be collected for specified, explicit purposes and not be processed further in a manner incompatible with the original purpose. The exceptions to this include where the data subject's consent must be obtained to reuse the data for another purpose or to comply with an obligation or function set out in law.

37. The inclusion of a **new list of processing purposes** which are automatically considered 'compatible' with the original purpose (**Part 1, clause 6**) could lead to reduced consumer control and transparency. According to our research, consumers value clarity and increased transparency about the precise purpose and use of their data, and a clear understanding of the relevant safeguards and data protection in place. As this list grows then consumers' data will be increasingly used in ways that they don't expect.

38. The current regime already makes appropriate provision for the re-use of data for public interest reasons. We believe that an extension of this approach could be to the detriment of consumers - with their data being reused in ways contrary to their expectations. The new list of 'compatible' purposes includes, at paragraph 10 of Annex 2, 'where the processing is carried out for the purposes of the assessment or collection of a tax or duty or an imposition of a similar nature'. This is vaguely worded and not linked to a specific statutory obligation to cooperate with a public authority such as HMRC. We therefore recommend that the Bill be amended to limit the application of this condition to processing carried out by public authorities in the performance of their tasks. We would also propose the deletion of paragraph 1 of Annex 2 as it is overly broad and does not set out a specific public interest.

39. In addition, there is another 'Henry VIII' power for the SoS to add to the new list of compatible purposes in Annex 2 by secondary legislation. This should not be done

without wide consultation that includes consumer representatives to ensure that consumer rights are respected. The government's proposed approach risks little or no scrutiny.

What we welcome

40. We welcome plans under **Part 3 of the Bill** to set up smart data frameworks for the use of consumer and business data. Smart data has the potential to bring greater choice and financial savings to consumers and increase competition between businesses to deliver better products and services. Open banking is the most well known version of smart data currently operating. Learnings from its implementation and how consumers have engaged with it must be factored into any expansion of the scheme. In particular, consideration must be given to the need to embed consumer protections including consent, control and transparency at the design stage of the schemes. Most of the detail will follow in secondary regulation and the government should commit to consulting on these proposals. Which? will work to influence the development of these frameworks, to ensure they work effectively for consumers, with the appropriate data protection safeguards in place.

41. We welcome the addition of a recognised legitimate interest of detecting, investigating or **preventing crime** (Annex 1). We believe that this could be useful for encouraging businesses to share important data for the purposes of preventing fraud. In paragraphs 11-13 we note that in order to encourage businesses to make use of this provision, the ICO must issue guidance on data sharing for the prevention of economic crime.

42. We welcome the proposal to expand the 'soft opt-in' rule to allow non-commercial organisations to use **electronic mail for direct marketing purposes (Part 4, clause 82)**, to contact people without consent if their details were obtained through them expressing an interest or supporting the objectives of the organisation. To ensure that this provision is not open to abuse and to protect vulnerable consumers from being subjected to spam, clear guidance must be provided by the ICO on the appropriate and proportionate use of the communication method. Proportionate and effective enforcement for rogue behaviour must also be pursued by the ICO.

43. We welcome introducing a duty for public electronic communication providers (someone who provides an electronic communications network or electronic communications service available for use by the public, such as broadband services) to notify the Commissioner of **unlawful direct marketing (Part 1, clause 85).** This should offer benefits to consumers, as it is likely to enable quicker sharing of intelligence, resulting in quicker enforcement action against companies causing harm to consumers. The proposed penalty of £1,000 should be significantly increased to deter organisations from non-compliance.

For more information, please contact publicaffairs@which.co.uk

May 2023