Data Protection and Digital Information (No.2) Bill

Written evidence submitted by Shoosmiths LLP to the House of Commons Public Bill Committee

10 May 2023

Introduction

This is a submission on behalf of the Privacy and Data team of Shoosmiths LLP (**Shoosmiths/we/us**) in response to the call for written evidence on the Data Protection and Digital Information (No.2) Bill (the **Bill**).

Shoosmiths is a law firm authorised and regulated by the Solicitors Regulation Authority under SRA number 569065. It is a limited liability partnership with registered company number OC374987 and its registered office is at 100 Avebury Boulevard, Milton Keynes MK9 1FH.

The Privacy and Data team at Shoosmiths is one of the UK's largest dedicated data protection and privacy teams working in private practice in the UK. It is recognised as a leading practice by the Legal 500 and UK Chambers legal directories. The team has many years of experience advising on data protection issues across many business sectors in the UK and globally. We advise the private sector, the public sector including regulators, and high-profile individuals.

We believe that our expertise will be valuable to the Committee in considering the detailed wording of the Bill.

References are as follows:

- **Bill**: Data Protection and Digital Information (No.2) Bill
- **DPA 2018**: Data Protection Act 2018
- **UK GDPR**: The General Data Protection Regulation (EU) 2016/679 as applicable in the UK
- **EU GDPR:** The General Data Protection Regulation (EU) 2016/679 as applicable in the EU
- **PECRs 2003**: Privacy and Electronic Communications (EC Directive) Regulations 2003/2426

(References to DPA 2018, GDPR and PECRs 2003 are given context within the narrative to indicate whether they are to the legislation as currently conceived, or as amended by the Bill.)

Executive Summary

- We support many of the Bill's reforms, in particular the greater flexibility given to organisations in their decisions about data subject access requests, impact assessments and records of processing activity.
- We have concerns about conflicting duties and objectives to be imposed on the Commissioner, the role of Senior Responsible Individuals, the powers of the Secretary of State with regard to the PECRs, and automated decision making.
- While international response to the Bill is difficult to predict, the very severe impact of withdrawal of the adequacy decision granted to the UK by the EU does, in our view, justify caution over some of the Bill's provisions, in particular the proposed transfer protocols and overall duties and objectives of the Commissioner.

Main text

1. **Duties of the Commissioner (Bill s.27; s.120B DPA 2018)**

    a. A general point of concern is the overwhelming likelihood of conflict between the principal objectives of the Commissioner in s.120A DPA 2018 and the new duties set out in new s.120B DPA 2018. Under the Bill, the interests of UK citizens are set in direct opposition to purposes specific to private enterprise and government. Although these latter purposes may be of indirect benefit to UK citizens, we would respectfully suggest that the existing duties (in current s.2(2)) should explicitly override the new duties. This would seem of particular importance bearing in mind the risk to UK adequacy arising from a wholesale departure from the aims of rights-based legislators, particularly in the EU.

    b. Of particular concern is the expansion of existing s.2(2) in new s.120A(b). The "promotion of public trust and confidence in the processing of personal data" should surely be the happy *effect* of good legislation, not a primary *aim*. It is not the job of the person tasked with protecting personal data to increase confidence that when processing takes place, it is always a good thing. Processing may be good or bad depending on context. We would suggest amending new s120A (b) to read "*by so doing* [i.e. by securing an appropriate level of protection], to promote public trust and confidence in the processing of personal data".

    c. The proposed duty to consult other regulators under s.120D is also likely to conflict with the Commissioner's other objectives in s.120A and 120B. The General Practice Data for Planning and Research (GPDPR) programme is a salutary lesson. An estimated 1.5 million people opted out of the programme after serious concerns were raised about privacy risks. The public voiced their concerns by opting out of to the programme aiming to bring innovation to healthcare. The Commissioner at the time also welcomed the delay of the launch. Should a future project of this nature be contemplated, the Commissioner must be able to exercise independence, not be prevented or influenced by consultation with other regulators or their own, conflicting, duties.

2. **DSARs - Vexatious and excessive requests (Bill s.7; Art.12A UKGDPR)**

    Proposed Art.12A provides organisations with a clear basis to refuse DSARs that are intended to cause distress, are not made in good faith or are a clear abuse of process. Although the factors determining "vexatious or excessive" in new s.204A are helpful, it is not clear why the factor in subsection 1(c) (resources of the recipient) is relevant to the determination. Whether requests are vexatious and excessive is an objective question based on the motives and actions of the sender, not the status of the recipient. It may be too tempting for recipients to base their assessment on their own lack of resources, rather than considering the requests in the round.

3. **Assessments of High Risk Processing (Bill s.17; Art.35 UK GDPR)**

a. We welcome the removal of the obligation to consult with data subjects before performing high-risk processing, and reconsideration of the requirement to carry out Data Protection Impact Assessments (DPIAs) in revised Art.35. These provide controllers with increased flexibility in the approach and format of identifying and managing privacy risk. However, as many organisations now have an embedded DPIA process, supported by external partners such as One Trust, that create automated DPIAs, this may not in practice change how large organisations conduct their risk assessments. This will be particularly the case for organisations which are at the same time achieving compliance with requirements under EU GDPR.

b. In the interests of accountability for organisations processing on the basis of Art.6(1)(c) and (e), we would suggest an additional requirement in revised Art.35(10) that any general impact assessment relied on for the purposes of that article is at least equivalent to any impact assessment which (but for that paragraph) would have been required under paragraphs 1 to 7.

4. **Records of Processing (Bill s.15; Art.30A UK GDPR)**

The changes will allow companies flexibility to comply with this obligation in a manner which is appropriate for their own processes and procedures; for example, if they are not processing high risk data. However, the changes in Arts. 30A 3(a) and 30A 6(b) will entail significant extra obligations for controllers and processors given the new obligations to keep a record of "where the personal data is (including information about any personal data that is outside the United Kingdom)". Clarification of whether this is intended to be only a location, include details of the identity of recipients, and an explanation of the words "information about" would be helpful. If retrospective, many organisations will need to update existing records to account for these changes.

5. **Senior Responsible Individual (SRI) (Bill s.14; Art.27A UK GDPR)**

a. We are concerned that the change in the name from Data Protection Officer (**DPO**) to SRI may result in unnecessary confusion as it does not indicate their relationship to data-related function.

b. A DPO is appointed on the basis of expert knowledge of data protection law and practice. A "senior responsible individual" requires neither, nor is required to have the relevant expertise. This change is therefore likely to lower the role's significance at a time when the importance of personal data processing and the risks involved could not be greater.

c. The new requirement in Art.27A(1)(b) UK GDPR for the private sector to appoint an SRI is broadened to any *high risk* processing. With fast-paced developments in technology, and in particular artificial intelligence, it is likely that many organisations, including start-ups, will need to appoint an SRI. While the new provisions will permit the SRI's tasks to be outsourced, the SRI will be expected to have their contact details available publicly (new Art.27A(4)(a)) which in the case of a start-up with outsourced data protection support, will result in added administrative burden to the SRI - who may also be the company founder.

d. Art.37(2) of current UK GDPR offers a *group of undertakings* the ability to appoint a single DPO. This option appears to be missing from the Bill. Clarification of the government's intention in this regard would be useful.

e. Under the existing regime, the same requirements for DPOs under the retained UK GDPR and EU GDPR provide consistency for businesses. UK organisations which offer services to EU clients and fall under the requirements of Art.37(1) EU GDPR will still be required to appoint a DPO. This could result in the need for the organisation to have separate roles: an SRI (who is a member of the organisation's senior management and is willing to carry this responsibility) and an independent DPO, resulting in further costs to the business.

f. Under proposed Art.27A(2)(c), the SRI will also be tasked with "informing *and advising* the controller, *any processor engaged by the controller* and employees of the controller who carry out processing of personal data *of their obligations under the data protection legislation*." This differs significantly from existing Art.39(a) UK GPDR and implies that controller's SRI may be required to provide data protection advice to its processor, with the risk of additional burden on the controller, ambiguity, and conflict of interest negotiating contracts with processors who may wish to rely on a controller for data protection advice.

6. Recognised legitimate interests (Bill s.5; Art.6 & Annex 1 UK GDPR)

a. The new "recognised legitimate interests" grounds of lawfulness processing, under Art. 6(1)(ea) and Annex 1 of UK GDPR, do not require the controller to consider or balance the countervailing interests, or rights and freedoms, of affected data subjects. We note that one of the recognised legitimate interests will be the detection, investigation or prevention of crime (under Annex 1, paragraph 5, of UK GDPR).

b. We have some concern about the possible impact of this in the context of CCTV usage. Specifically, we would suggest that the installation and use of CCTV, including adoption of advanced CCTV technologies (such as facial recognition), must remain subject to balancing considerations as to placement, usage, sharing and so on.

c. In addition, we are concerned that the fact that prevention/detection of crime will be a recognised legitimate interest might in practice put controllers of CCTV footage under increased pressure to share footage voluntarily with police forces or other law enforcement authorities. In this respect it is not clear how new Article 6(1)(ea) is intended to operate in the context of the substantial public interest condition at paragraph 10, Schedule 1 DPA 2018, which also requires any voluntary sharing of CCTV footage with police forces to be necessary for reasons of "substantial public interest". Without further guidance, we are concerned that the addition of the prevention/detection of crime as a "recognised legitimate interest" will enable police forces to argue that it is always in the substantial public interest for criminal

offence data to be shared with them. We would recommend further guidance or constraints on this point.

7. **PEC Regulations – Statistical and analytics cookies (Bill s.79; PECRs s.2A(b))**

Allowing cookies to be used for the "sole" purpose of statistical and analytics on an opt-out basis is a progressive change and will align the UK to other expanding privacy regimes, such as US state privacy laws. However, much of the technology currently used to gather such information also tends to gather unique identifiers relating to the user or their device (e.g. the device name, IP address etc.) despite such information being unnecessary for the intended purpose, which is the statistical counting or analysis of how a particular website or service is being used. Technology is already readily available to allow such statistical and analytical activities to occur on an anonymous basis. Such statistical and analytical data can give valuable insight into the browsing habits of users and we have regularly seen cases of such information being leveraged for wider audience insights, profiling and engagement activities, which are subject to opt-in consent. Therefore, we would advocate for a caveat to be added to the "(2A)(b) exception" that the exception shall only apply where such storage or access does not involve the collection or processing of any other identifiers.

8. **PEC Regulations - Secretary of State's powers to amend (Bill s.79(3); PECR s.6A (1))**

Although allowing the Secretary of State (SoS) to change the essential, non-essential (opt-out) and non-essential (opt-in) categories will allow the reformed PECRs to keep pace with future developments and public understanding of harm-based privacy regulation, we feel that this power is better placed with the Commissioner or perhaps the Digital Regulation Cooperation Forum (DRCF). Arguments about cookies - particularly the frequency of cookie pop-ups – have preoccupied regulators for many years, but few solutions have been put forward that do not materially affect user privacy rights. We would therefore suggest that this power is conferred on the appropriate regulators or, alternatively, that the SoS will only use its power "to reflect guidance issued by [the appropriate regulators]".

9. PEC Regulations - Secretary of State's powers of prohibition (Bill s.79(3); PECR s.6B)

We note the SoS's new power to prohibit browser/device suppliers from supplying certain types of technology unless it meets the requirements specified in the regulations. Widening the scope of compliance to encompass organisations supplying technology is a welcome change, since businesses processing cookie-derived data are often at the mercy of the technical limitations imposed upon them by suppliers. However, we would respectfully argue that such powers already exist and, as with 6A(1), is better placed in the hands of the appropriate regulators (i.e., the Commissioner and/or DRCF). The Commissioner already maintains a certification mechanism, under which it could establish technologically agnostic parameters which meet the requirements specified under the amended PECRs. The Commissioner's work on certification schemes has proved successful in areas such as age-gating and age-appropriate design. Finally, in supporting existing mechanisms – as opposed to conferring new powers – the proposed s.6B can take a proactive rather than reactive approach to regulation.

10. **Automated decision making (Bill s.11; Art.22A UK GDPR)**

a. The Bill effectively abolishes the general prohibition on automated decision making (ADM) under Art.22 UK GDPR. This proposal diverges materially from other privacy regimes, and runs counter to the Government's own response to its data consultation where it acknowledges that "the right to human review of an automated decision was a key safeguard".

b. Particular problems with this approach are:

    i. Confining the general prohibition to "special personal data", since the majority of use-cases where ADM has proven controversial are not restricted to this type of data, such as social engineering, credit risk scoring, cost profiling and educational decisions (see for example, recent problems over A-level marking algorithms).
    ii. The concept of a "significant decision" test provides little safeguard for data subjects as there is no threshold as to what constitutes a "significant decision", determinations are likely to be highly subjective and risk exploitation for commercial gain, and may render redress ineffective by adding a burden of proof on data subjects to demonstrate that a determination made by a controller was incorrect.
    iii. We support attempts to reduce the burden on businesses conducting routine or non-intrusive ADM but would strongly urge a reconsideration of the current proposal. Recent developments in generative AI mean that the risks from ADM are increasing and support further regulation, not less.
    iv. We would suggest a "white-list" approach, whereby those use-cases widely understood to be low risk and nonintrusive could benefit from an exception.

11. **International transfers: the data protection test (Bill s.21 and Schedule 5, Art.45B UK GDPR)**

The new 'data protection test' (which appears to replace the current Transfer Risk Assessment framework) is more business-friendly and will allow data to transfer more freely to non-adequate countries. However, we suspect this may have an impact on the EU's adequacy decision in favour of the UK. The particular concern for the EU will be that the data protection test will require that an importer's standard of data protection is not 'materially lower' than the protections granted under UK law. Given that the Bill will reduce the standard of compliance in the UK, meeting the UK's level of compliance may be too low a standard for the EU. In our view, the economic benefit of being able to export data more freely to non-adequate countries is likely to be outweighed by the economic detriment of losing EU adequacy status.

12. **International transfers: Responsibility for the data protection test (Bill s.21 and Schedule 5, Art.46 UK GDPR)**

Under the redrafted Art.46 UK GDPR (and specifically under new Art.46(1A)(a)(ii), and new Art.46(6)), there is no explanation of who conducts a data protection test. It would make practical sense for the exporter to conduct the test, with the importer providing the relevant

information set out in Art.45B(2), as they will be in a better position to provide details relating to relevant impacting laws and practices.