PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Recommendations on the Data (Use and Access) Bill

1 Part 1: Access to customer data and business data

#	Topic	Reference in Bill	Relevant text in Bill	Comment
1	Customer data and business data	Clause 1(2) and Clause 25(1)	***1*** *(2) In this Part—* *"business data", in relation to a trader, means—* *(a) information about goods, services and digital content supplied or provided by the trader,* *(b) information relating to the supply or provision of goods, services and digital content by the trader (such as, for example, information about—…* *…* *"customer data" means information relating to a customer of a trader, including—* *(a) information relating to goods, services and digital content supplied or provided by the trader to the customer or to another person at the customer's request (such as, for example, information about—…* *…* ***25*** *(1) "digital content" means data which is produced and supplied in digital form;*	Business data includes "digital content", which the Bill defines as "data… produced and supplied in digital form". We are concerned that the data access provisions in Part 1, to the extent they require the provision of digital content, could impinge on editorial freedoms of journalistic activities. Those freedoms and activities are protected under other legislation that compels the provision of data. For example, the subject access right in the UK GDPR is subject to a broad exemption in respect of personal data held or processed for the purposes of journalism, art or literature (the so-called special purposes). One possible approach to remediate this gap in the Bill, would be to carve out, from the scope of the data regulations, any requirement to provide customer or business data processed in the course of, or held for the purposes of, a "content service" within the meaning of s. 32(7) of the Communications Act 2003. This definition is relied on in other contexts, for example equality legislation.

#	Topic	Reference in Bill	Relevant text in Bill	Comment
2	Interface bodies – eligibility criteria, interoperability	Clause 7(1)-(2)	***Interface bodies*** … *(4) In relation to an interface body (whether or not it is required to be set up by regulations under section 2 or 4), the regulations may—* *(a) make provision about the body's composition and governance;* *(b) make provision requiring a data holder or a third party recipient to provide, or arrange for, assistance for the body;* *(c) impose other requirements relating to the body on a person who is required to set it up or to provide, or arrange for, assistance for the body;* *(d) make provision requiring the body to carry on all or part of a task described in subsection (1);* *(e) make provision requiring the body to do other things in connection with its interface, interface standards or interface arrangements;* *(f) make provision about how the body carries out its functions (such as, for example, provision about the body's objectives or matters to be taken into account by the body);* *(g) confer powers on the body for the purpose of monitoring use of its interface, interface standards or interface arrangements ("monitoring powers") (and see section 8 for provision about enforcement of requirements imposed in exercise of those powers);* *(h) make provision for the body to arrange for its monitoring powers to be exercised by another person;* *(i) make provision about the rights of persons affected by the exercise of the body's functions under the regulations, including (among other things)—*	(1) In our view the Bill should set out minimum eligibility criteria for 'interface bodies'. For example, we would expect interface bodies to need to be established in the UK. This will help ensure that interface bodies can be effectively regulated. This does not impede international data flows, as the interface bodies may still share information internationally (whether under UK GDPR or otherwise) in the usual way. (2) Furthermore, we think the Bill would benefit from setting out a framework for determining the types of data that can be shared (for example value judgements should not be shareable but maybe simply facts – some value judgements may represent valuable IP) and who the data can be shared with, rather than leaving these important matters to be dealt with by future data regulations only. (3) The Bill should also compel the various 'interface bodies' that will exist (as it is possible for there to be multiple such bodies) to work together to align their services and approaches to facilitate interoperability (for example, between their respective APIs) in the long-term. Alternatively, the Secretary of State or Treasury could be given the power to require this. This will minimise the risk that the interface bodies create new data

#	Topic	Reference in Bill	Relevant text in Bill	Comment
			(i) provision about the review of decisions made in exercise of those functions; *(ii) provision about appeals to a court or tribunal;* *(j) make provision about complaints, including provision requiring the body to implement procedures for the handling of complaints;* *(k) make provision enabling or requiring the body to publish, or provide to a specified person, specified documents or information relating to its interface, interface standards or interface arrangements;* *(l) make provision enabling or requiring the body to produce guidance about how it proposes to exercise its functions under the regulations, to publish the guidance and to provide copies to specified persons.*	siloes that cannot interact with each other.
3	Investigations and Enforcement under Part 1	Clause 9	*(3) Information is within this subsection if it is information in respect of which ~~a communication which is made~~—* *~~(a) between a professional legal adviser and the adviser's client, and~~* *(a) a claim to legal professional privilege or, in Scotland, confidentiality of communications, could be maintained in legal proceedings, or* *~~(b) in connection with the giving of legal advice to the client with respect to obligations, liabilities or rights imposed or conferred by or under regulations made under this Part.~~* *(b) a duty of confidentiality is owed by a professional legal adviser to a client of the adviser.* *(4) Information is within this subsection if it is information in respect of a communication which is made—* *(a) between a professional legal adviser and the adviser's client or between such an adviser or client and another person,*	Clause 8(4) provides for a wide and unfettered power to compel "provision of documents or information". The exemptions under Clause 9 in respect of privilege are narrow, covering only (i) legal advice given in relation to this Part of the Bill (Clause 9(3)(b)) and proceedings arising out of this Part of the Bill (Clause 9(4)(b-c)). It is not clear why privileged advice in relation to other legislation that interacts with this legislation (such as the portability right under GDPR or access rights under FOIA or the EIR) should be disclosable. One way to deal with this would be to align the Clause 9(3) provision on legal professional privilege with the wording of

#	Topic	Reference in Bill	Relevant text in Bill	Comment
			(b) in connection with, or in contemplation of, proceedings ~~under or arising out of regulations made under this Part (including proceedings arising out of the exercise of powers conferred by such regulations)~~, and *(c) for the purposes of such proceedings.*	paragraph 19 (*Legal professional privilege*), Schedule 2 of the Data Protection Act (the "DPA") 2018. We have suggested amendments in green accordingly.
4	Restrictions on processing and data protection – exemptions for private sector	Clause 20	***Restrictions on processing and data protection*** *(1) Except as provided by subsection (2), regulations under this Part may provide for the processing of information in accordance with the regulations not to be in breach of—* *(a) any obligation of confidence owed by the person processing the information, or* *(b) any other restriction on the processing of information (however imposed).*	Clause 18 of the Bill permits the Secretary of State or the Treasury to make regulations to exempt a public authority from liability when they exercise their functions under Part 1 of the Bill. By contrast, when the private sector organisation is carrying out obligations pursuant to Part 1 of the Bill, Clause 20 of the Bill only permits regulations to exempt an organisation from a breach of the duty of confidence or other restriction on the "processing" of information. That list purports to be exhaustive. We expect that private sector organisations, and quasi-public organisations will be concerned about other types of liabilities too when they are required to share information. For example, liabilities arising from Intellectual Property Rights infringements (for example in respect of copyright works or sui generis rights in databases) and obligations under contracts with third parties. Accordingly, our view is that this Clause should be broadened so that it is equivalent in scope to Clause 18, or at

#	Topic	Reference in Bill	Relevant text in Bill	Comment
				the very least contain a non-exhaustive list of “such other liabilities as maybe reasonable in the circumstances”.

2 Part 5: Data protection and privacy

#	Topic	Reference in Bill	Relevant text in Bill	Comment
5	Meaning of research and statistical purposes – scientific research	Clause 67(1)(b)	*(2) References in this Regulation to the processing of personal data for the purposes of scientific research (including references to processing for "scientific research purposes") are references to processing for the purposes of any research that can reasonably be described as scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity.* *(3) Such references* *(a) include processing for the purposes of technological development or demonstration, fundamental research or applied research, so far as those activities can reasonably be described as scientific, but* *(b) only include processing for the purposes of a study in the area of public health that can reasonably be described as scientific where the study is conducted in the public interest.*	(1) We think the Bill would benefit from a non-exhaustive list of activities or criteria for 'scientific research' (which would be clearly marked as non-exhaustive). Non-exhaustive examples of activities might include, for example, clinical trials, and non-exhaustive criteria might be imported from relevant ICO guidance available here. These example activities / criteria must not prejudice the broad definition of 'scientific research' purposes in the Bill. (2) Furthermore, reflecting the government's priorities, this Clause of the Bill could specifically recognise as in the public interest (i) the processing of personal data by or on behalf of the NHS and/or (ii) the use and/or improvement of technology by the NHS, in each case in furtherance of reforming or improving NHS health and care services. (3) As a matter for further clarification or guidance, which could be addressed in the explanatory notes for example, how will the definition of scientific research be interpreted in the context of the use of AI systems? For example, what steps are needed at the start and end of research that involves the use of AI? When should such research be peer reviewed? These could be matters that will be appropriately addressed in ICO guidance or an ICO code of practice.

#	Topic	Reference in Bill	Relevant text in Bill	Comment
				(4) Finally, we think it would be helpful to be clear that the *application* of epidemiological scientific research which has been carried out in compliance with this research ground, perhaps in the context of treatment in the NHS only (reflecting the government's priorities) should not require renotification or consent from patients under the UK GDPR. Without this, the value of the scientific research exemption, is very significantly diminished as it may be impossible to use data to deliver treatments, that the same data in research has identified will deliver clinical benefits to patients. Put another way, if the scientific research is in the public interest, then the use of the same data to treat patients must also be in the public interest. Note that the current vital interests grounds in the UK GDPR is not applicable, as you may need to process data of many prior patients, in order to treat a new patient (and not just the data of the patient being treated).
6	Power of the Commissioner to require a report – expert approval process	Clause 97(3)	***After section 146 insert***— ***"146A Assessment notices: approval of person to prepare report etc*** *(1) This section applies where an assessment notice requires a controller or processor to make arrangements for an approved person to prepare a report.* *(2) The controller or processor must, within such period as is specified in the assessment notice, nominate to the Commissioner a person to prepare the report.*	(1) Section 146A(4) provides that if the ICO is not satisfied with the nominated person, it must approve an alternative expert who the ICO is satisfied is a suitable person. That process begs the question 'how will the ICO-approved suitable person be identified?' We would expect a step to be included before this approval by the ICO of their suitable person, where the controller or processor would discuss alternative people with the ICO

#	Topic	Reference in Bill	Relevant text in Bill	Comment
			(3) If the Commissioner is satisfied that the nominated person is a suitable person to prepare the report, the Commissioner must by written notice to the controller or processor approve the nominated person to prepare the report. *(4) If the Commissioner is not satisfied that the nominated person is a suitable person to prepare the report, the Commissioner must by written notice to the controller or processor—* *(a) inform the controller or processor that the Commissioner has decided not to approve the nominated person to prepare the report,* *(b) inform the controller or processor of the reasons for that decision, and* *(c) approve a person who the Commissioner is satisfied is a suitable person to prepare the report to do so.* *(5) If the controller or processor does not nominate a person within the period specified in the assessment notice, the Commissioner must by written notice to the controller or processor approve a person who the Commissioner is satisfied is a suitable person to prepare the report to do so.*	(giving the controller or processor an opportunity to identify these alternatives and make representations as to their suitability) before the ICO approves their suitable person. (2) As a matter for clarification, please confirm whether the suitable person can be an internal employee of the controller or processor, such as the DPO, or whether they must be an external party. We would welcome this clarification preferably in the Bill itself, alternatively by way of ICO guidance. (3) Given that the controller or processor is financially liable to pay for the expert report, and noting the consequences of failing to comply with an assessment notice, we expect a process to be included for the controller or processor to submit representations on the terms of reference of an expert report, whereby the ICO will take account of the controller or processor's views when discharging its powers.
7	Storing information in terminal equipment	Clause 111 and Schedule 12	*111 (6). —(1) Subject to Schedule A1, a person must not store information, or gain access to information stored, in the terminal equipment of a subscriber or user.* *(2) In paragraph (1) and Schedule A1—* *(a) a reference (however expressed) to storing information, or gaining access to information stored, in the terminal equipment of a subscriber or user includes a reference to instigating the storage or access, and*	(1) There appears to be a misalignment between the scope of the prohibition in Clause 111 and the proposed exemptions to that prohibition in Schedule 12 (new Schedule A1), sections 4 to 7. The prohibition in Clause 111 applies to *any* type of access to *any* terminal equipment. However, the exemptions only apply in respect of the provision of information society

#	Topic	Reference in Bill	Relevant text in Bill	Comment
			(b) except as otherwise provided, a reference (however expressed) to gaining access to information stored in the terminal equipment of a subscriber or user includes a reference to collecting or monitoring information automatically emitted by the terminal equipment."	services ("**ISSs**"). In practice, not all internet operations are ISSs. (2) Some of proposed exemptions require the subscriber to be given a simple means of objecting to the storage or access (see for example para 5(1)(e), Schedule 12). A number of points arise here: - Please clarify the standard or means for that objection right, for example should the right be offered in a pop up or consent management platform on the site itself at the time the processing takes place? - Would it be appropriate to rely instead on a right to opt out by way of email or separate communication from the user? - The opt out should expressly apply to processing of information gathered in the future. Unpicking information already gathered under this right will be a disproportionate task. If an individual has not exercised their opt-out right for (say) three years, and then chooses to exercise that right, retrospective application of the opt-out strikes the incorrect balance between the individual and business. The individual can exercise their rights at any time; their choice to wait should not prejudice the organisation. (3) With reference to the inclusion of the words "automatically emitted" in Clause 111(6)(b), has technical input been obtained in relation to the breadth of the prohibition as a result of the use of those words? We are

#	Topic	Reference in Bill	Relevant text in Bill	Comment
				concerned, for example, that from a technical perspective, a broader range of data emitted from a de-vice would be caught by the provision than the legislature has anticipated. For example, static IPv4 addresses and IPv6 addresses would be caught as they are retrieved from the terminal equipment and are not, like CGNAT IP addresses, generated by the network. URL tracking links would also be caught as these must be stored on the memory of the device before the URL link is clicked on the user. The consequence is that the processing of that information – unless 'strictly necessary' or otherwise exempt under Schedule 12 – can only take place on the basis of consent but it is not clear in many cases how consent can be obtained by the publisher in practice.
8		Schedule 12 para 5(1)(b)	*(b) the sole purpose of the storage or access is to enable the person—* *(i) to collect information for statistical purposes about how the service is used with a view to making improvements to the service, or* *(ii) to collect information for statistical purposes about how a website by means of which the service is provided is used with a view to making improvements to the website, …*	(1) We would welcome clarity, preferably in the Bill itself, in relation to the meaning of "statistical purposes" in this paragraph. Do "statistical purposes" include web-site analytics? Can those analytics be carried out by a third party e.g. through the use of Google Analytics? (2) It seems to us that the "sole purpose" test would prevent publishers from using multipurpose exempt cookies – i.e. one cookie would be needed for analytics, and another one for website appearance etc. A possibly better alternative would be to state that these activities are deemed to be "strictly

#	Topic	Reference in Bill	Relevant text in Bill	Comment
				necessary" for the purposes of the exemption in Schedule 12 para 4(2).
		Schedule 12 para 5(2)	*… In sub-paragraph (1), the reference to gaining access to information stored in the terminal equipment of a subscriber or user does not include a reference to collecting or monitoring information automatically emitted by the terminal equipment.*	The reason for the carve out for automatically emitted information is not clear to us and risks undermining the exemption in Schedule 12 para (5)(1).
		Schedule 7(6)(6)-(7)	*6. For the purposes of this Article, the data protection test is met in relation to a transfer, or a type of transfer, of personal data if, after the transfer, the standard of the protection provided for the data subject with regard to that personal data by the safeguards required under paragraph 1A, and (where relevant) by other means, would not be materially lower in practice than the standard of the protection provided for the data subject with regard to the personal data by or under—* *(a) this Regulation,* *(b) Part 2 of the 2018 Act, and* *(c) Parts 5 to 7 of that Act, so far as relevant to processing to which this Regulation applies.* *7. For the purposes of paragraph 1A(a)(ii) and (b)(ii), what is reasonable and proportionate is to be determined by reference to all the circumstances, or likely circumstances, of the transfer or type of transfer in practice, including the nature and volume of the personal data transferred.*	Please incorporate the wording 'in practice' (shown in green), which was important in the Schrems II judgment. This is because it should be clear that it is not simply a question of whether access to the data by the state in the country of import is possible *in theory* under local law, but that other relevant factors can include the circumstances in which that access takes place in practice as well as other matters relating to the importer's operations and the technical ability for the state to gain access to the imported data.

3 Part 6: The Information Commission

#	Topic	Reference in Bill	Relevant text in Bill	Comment
9	The Information Commission - membership	Schedule 14 para 2(2)	*2(1) The number of members of the Commission is to be determined by the Secretary of State.* *(2) That number must not be—* *(a) less than 3, or* *(b) more than 14.*	We think the upper limit for the number of members of the Commissioner in para 2(2)(b) should be reduced to 10. That is because any more than 10 would, in our view, lead to inefficient decision-making (and that has been the experience in other jurisdictions where very large commissions exist).

#	Topic	Reference in Bill	Relevant text in Bill	Comment
10	The Information Commission – appointment to membership	Schedule 14 para 3 and 5	***Membership: general*** *3 (1) The Commission is to consist of—* *(a) the non-executive members, and* *(b) the executive members.* *(2) The non-executive members are—* *(a) a chair appointed by His Majesty by Letters Patent on the recommendation of the Secretary of State, and* *(b) such other members as the Secretary of State may appoint.* *(3) The executive members are—* *(a) a chief executive appointed by the non-executive members or in accordance with paragraph 25, and* *(b) such other members, if any, as the non-executive members may appoint.* *(4) The Secretary of State must consult the chair of the Commission before appointing a non-executive member.* *(5) The non-executive members must consult the Secretary of State* *before appointing the chief executive.* *(6) The non-executive members must consult the chief executive about whether there should be any executive members within*	(1) While we are conscious that these appointments would likely follow the normal process for public appointments, in other jurisdictions such as France nominations for members of the Commission are sought from specific groups in order to ensure a minimum level of diversity. It would be beneficial to allow, for example, for nominations to be invited from the TUC, CBI, Charity Commission and so on.

#	Topic	Reference in Bill	Relevant text in Bill	Comment
			sub-paragraph (3)(b) and, if so, how many there should be. *(7) The Secretary of State may by direction set a maximum and a minimum number of executive members.* *(8) The Commission may appoint one of the non-executive members as a deputy to the chair.* ***Membership: selection on merit etc*** *5 The Secretary of State may not recommend a person for appointment as the chair of the Commission unless the person* *(1) has been selected on merit on the basis of fair and open competition.* *(2) A person may not be appointed as a member of the Commission unless the person has been selected on merit on the basis of fair and open competition.*	
11	The Information Commission – decision-making	Part 6 and Schedule 14	N/a	As a matter for clarification, please explain how decision-making will work within the ICO after the restructuring into a body corporate that is proposed under this Part. Will overall responsibility for key matters still be a matter for the Chair?

#	Topic	Reference in Bill	Relevant text in Bill	Comment
12	The Information Commission – principal objective	Clause 90 (120A)	*It is the principal objective of the Commissioner, in carrying out functions under the data protection legislation—* *(a) to secure an appropriate level of protection for personal data, having regard to the interests of data subjects, controllers and others and matters of general public interest, and* *(b) to promote public trust and confidence in the processing of personal data.*	(1) Please add 'processors' to sub-section a, or explain why they are omitted from the sub-section. (2) Please add a provision that would require the Commission to be transparent in relation to how it prioritises its primary objective while balancing its duties under section 120B.
13	The Information Commission – duties	Clause 90 (120B)	*In carrying out functions under the data protection legislation, the Commissioner must have regard to such of the following as appear to the Commissioner to be relevant in the circumstances—* *(a) the desirability of promoting innovation; (b) the desirability of promoting competition;* *(c) the importance of the prevention, investigation, detection and prosecution of criminal offences;* *(d) the need to safeguard public security and national security;* *(e) the fact that children may be less aware of the risks and consequences associated with processing of personal data and of their rights in relation to such processing.*	As a matter for clarification, please explain the reasoning behind these duties and how they were determined. In particular, these appear to contain some aspects of the Growth Duty under the Deregulation Act 2015 (innovation for example), but not all aspects. It is not clear how the Growth Duty and these principal and secondary objectives interact.