GDPR Implementation Series

United Kingdom: Heading Towards Brexit but with a Data Protection Bill Implementing GDPR

*Lorna Woods**

I. Introduction

Following on from its Statement of Intent, the British Government has published the Data Protection Bill with the intention of meeting the European Union General Data Protection Regulation¹ (GDPR) timing of May 2018. After Brexit, the GDPR will be incorporated into the UK's domestic law under the EU (Withdrawal) Bill, currently before the UK Parliament.² One of the key concerns of the UK Government³ is to ensure that the UK gets an adequacy agreement by trying to ensure the Data Protection Bill (the DP Bill)⁴ provides a 'broadly equivalent' level of protection to the GDPR.⁵ It remains to be seen if such a regime is 'essentially equivalent'.⁶ The DP Bill is currently being considered by the House of Lords before going to the Commons and it does not look like royal assent is possible this year.

II. Structure of the Data Protection Bill

The DP Bill is not only long but also complex. It contains seven parts, each sub-divided into chapters, and

18 schedules. Schedules follow the main text of the relevant act and, while much of the content is technical detail, schedules can contain important provisions. This is the case here. The DP Bill aims to do four things:

- Filling in the legal spaces allowed by the GDPR (Part 2, Chapter 2 as well as Schedules 1-5);
- Setting up a system which applies where EU law does not which effectively means the post-Brexit system but also public authorities who hold unstructured manual files (Part 2, Chapter 3 together with Schedule 6);
- Implementing the Law Enforcement (or: Police) Directive⁷ (Part 3 together with Schedule 7 and 8); and
- Providing data protection rules for the intelligence services (Part 4 together with Schedules 9-11).

Cross-cutting provisions – notably the powers of the Information Commissioner's Office (ICO)⁸ and matters relating to enforcement – are found in Parts 5 and 6 and Schedules 12-16 of the DP Bill. Part 7 (and

DOI: 10.21552/edpl/2017/4/12

* Lorna Woods, Professor of Internet Law, School of Law and Human Rights Centre, University of Essex. The views expressed are the author's own and are not representative of the University of Essex. For correspondence: <lmwoods@essex.ac.uk>.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

2 cl 3 EU (Withdrawal) Bill, though arguably the way cl 19(1) Data Protection Bill is drafted means that at least ch 3 to pt 2 could apply in any event, as it applies to 'an activity which is outside the scope of European Union law....'.

3 See generally, HM Government, 'The exchange and protection of personal data: A Future Partnership Paper.' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf> accessed 24 November 2017.

4 Data Protection Bill (HL Bill 66) <https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/lbill_2017-20190066_en_1.htm> accessed 24 November 2017; for overview information also <<https://www.gov.uk/government/collections/data-protection-bill-2017>> accessed 24 November 2017.

5 cl 3(3)(b) Data Protection Bill. Cf an earlier Practitioner's Report in which the possible avenues for the UK in view of the GDPR were discussed Lokke Moerel and Ronan Tigner, 'Data Protection Implications of "Brexit"' (2016) 2(3) EDPL 381-383.

6 Case C-362/14 *Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, para 73.

7 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L119/89.

8 For more information <<https://ico.org.uk/>> accessed 24 November 2017.

Schedules 17-18) contains miscellaneous matters, including offences and territorial scope. This report considers – and points out the problems of – those aspects of the DP Bill relating to the GDPR and the post-Brexit position, but not the parts dealing with the Law Enforcement Directive or the intelligence services (though they too would be relevant to any assessment on adequacy of the UK with EU data protection standards).

Given the range of tasks the DP Bill attempts to address, perhaps its length is only to be expected, although we might question why the intelligence services should be treated so differently from law enforcement. The fact that an EU Regulation should not be implemented in domestic law also makes drafting difficult in relation to exemptions and aspects where further detail by national legislatures is permitted by the GDPR. Here, the DP Bill needs to be read alongside the GDPR. Notwithstanding these factors, the DP Bill is open to criticism for being unnecessarily complicated, containing clauses which – while they do have meaning – on first reading seem ridiculous⁹, and by continuing the ‘split’ structure found in the Data Protection Act 1998 (DPA 98)¹⁰, which hived off central aspects of the law to various schedules, rather than expressing those provisions in the main body of the act.

III. Overview of Especially Relevant Provisions

1. Rules on Consent and Other Processing Justifications

In terms of children and information society services, the Government has exercised its right to lower the age of consent to 13 (where Article 8 GDPR mentions the age of 16 with the right to choose a lower age by Member States down to 13 years)¹¹, and specifies that the ‘reference to “information society services” does not include preventative or counselling services’.¹² This reference is found in the recitals to the GDPR and so might be a legitimate limitation of ‘information society services’.¹³ Nonetheless, this leaves us in the odd position that a (non-binding) recital is used as the basis for domestic law amending the meaning of a different piece of EU legislation. The DP Bill may not be the only piece of legislation that relies on this type of ‘clarification’ to include specific provision in national law. Nonetheless, the DP Bill does not define what is meant by such services. We might question how this group of service providers relates to other services in the field of health and social work: are they the same sort of actors or different?

While the conditions for processing are set down in the GDPR, Article 6(1) GDPR allows Member States to make more specific rules regulating the processing of data for public interest purposes. Article 6(1)(f) cannot be relied upon to justify data processing by public authorities in the performance of their public tasks. The definition of a ‘public authority’ is therefore important but is not defined in the GDPR. The DP Bill defines ‘public authority’ and ‘public body’, in a manner consistent with the DPA 98:

- (a) it is a public authority under the Freedom of Information Act 2000 (FoI) (or its Scottish counterpart), or
- (b) it is designated a public authority under a separate regulation.¹⁴

On the face of it, this means that publicly-owned companies, which under the FoI are seen as public authorities, will not be able to take the benefit Article 6(1)(f) GDPR. A couple of further points should be noted. First, the statement in (a) may be changed by regulation made by the Secretary of State, either to expand the group of public bodies, or to make it smaller. Secondly, the DP Bill contains more detail regarding law-

9 See eg, cl 4 DPB which states ‘Terms used in Chapter 2 and in the GDPR have the same meaning in Chapter 2 as they have in the GDPR’; 4(1) points out ‘In subsection (1), the reference to a term’s meaning in the GDPR is to its meaning in the GDPR read with any provision of Chapter 2 which modifies the term’s meaning for the purposes of the GDPR’; 4(2) continues ‘Subsection (1) is subject to any provision in Chapter 2 which provides expressly for the term to have a different meaning’.

10 Available at <<https://www.legislation.gov.uk/ukpga/1998/29/contents>> accessed 24 November 2017.

11 The ICO had previously said in guidance that a child under 12 was unlikely to be competent to consent, which is also the position in Scotland – see cl 187; it seems according to the Lord Bishop of Chelmsford that the rationale for this choice is the convenience of social media companies: Hansard, 10 October 2017, col 139 <[https://hansard.parliament.uk/Lords/2017-10-10/debates/22188EC1-6BAB-4F06-BE64-5831ABAF78E2/DataProtectionBill\(HL\)#contribution-CA6F4535-F965-4D3A-B6EB-5328BD4CA9C6](https://hansard.parliament.uk/Lords/2017-10-10/debates/22188EC1-6BAB-4F06-BE64-5831ABAF78E2/DataProtectionBill(HL)#contribution-CA6F4535-F965-4D3A-B6EB-5328BD4CA9C6)> accessed 24 November 2017.

12 cl 8(b) DP Bill.

13 recital 38 GDPR.

14 cl 6 DP Bill.

ful processing in the public interest by listing examples of such processing. It should be noted, however, that this list is a non-exhaustive list.¹⁵ This form of drafting suggests that public authorities can then process data on other grounds, not listed in the DP Bill, and raises the question of which grounds would be acceptable.¹⁶ Lord Patel suggested that the Government intended that the non-exhaustive nature of Clause 7 would allow, for example, research conducted by universities or the National Health Service trusts to use the public interest legal basis.¹⁷ Presumably, the outer edges of the possible grounds are defined by the terms of Article 6(1)(e) (ie necessary for a task in the public interest or in the exercise of the controller's official authority), but who decides this point: the public authorities themselves? Is this an attempt by the drafters to mitigate the impact of the exclusion of public authorities from relying on Article 6(1)(f)?

2. Special Categories of Data and Processing

Clause 9 deals with special categories of data and specifies the conditions in which processing may be said to be on the basis of law in the context of Article 9(2)(b)(g)(h)(i) and (j).¹⁸ This means a condition from Schedule 1 to the DP Bill must be met, in addition to a condition from Article 6 GDPR. This part of the DP Bill lacks the detail found in Schedule 3 to the DPA 98, which contained the provisions for processing of sensitive data in accordance with the Data Protection Directive. It is however equivalent: the 'missing' provisions derive from the direct applicability of the GDPR. The DP Bill requires that certain acts of processing must satisfy the 'additional safeguards' found in Part 4 to Schedule 1, which requires a policy document (as envisaged under Article 30(1)(e) and 30(2)(c) GDPR) to be in place. While 'substantial public interest' may under the GDPR justify the processing of such data, there is no definition of this term – or even, more generally, of the idea of public interest. This is a not uncommon failing in legislation. Under Clause 10(2) and Schedule 1 of the DP Bill, provision is made to permit employers to process criminal convictions data as part of their pre-employment checks, and insurers can process criminal convictions data for anti-fraud purposes. The stated policy aim was to ensure that all 'special category' processing currently carried out in reliance on Schedule 3 DPA

98 in relation to 'sensitive personal data' can continue; in pursuance of maintaining the status quo, the processing in relation to Clause 10 is subject to similar conditions to those found in Article 9(2) GDPR.

Clause 12 specifies the specific obligations of credit reference agencies¹⁹ in an adaptation of Section 9(2) DPA 98. It adjusts the obligation of the controller when responding to a subject access request²⁰ to mean a request 'only to personal data relating to the data subject's financial standing, unless the data subject has indicated a contrary intention'.²¹ This does not, of course, defeat the data subject's rights but it does not seem entirely at one with the idea of transparency. Admittedly, Recital 63 GDPR recognises that a controller may ask the data subject to specify information when the data controller holds large quantities of data. Clause 12, however, is not based on quantity but rather the type of controller. The inclusion of such a presumption may mean that the data subject does not know that the controller might hold still more personal data and that the data subject can ask for that.

Clause 13 deals with automated decision-making, specifically Article 22(b) GDPR. It has similarities to the approach taken in Section 12(2) DPA 98. Decisions within Article 22(2)(b) are 'qualifying significant decisions'. The DP Bill allows qualifying significant decisions, based solely on automated processing, subject to certain safeguards: the notification of the individual concerned; and the right of this individual to request the data controller to reconsider its decision or make a decision not using automated decision-making.²² Whether these safeguards are sufficient is open to question, especially as regards special categories of personal data which do not generally fall within Article 22(2) but which are not excluded by the DP Bill (see Article 9).

¹⁵ Explanatory Notes, para 86.

¹⁶ The DPA 98, implementing the Data Protection Directive, has an exhaustive list in para 5 of sch 2.

¹⁷ Lord Patel, Hansard, 10 October 2017, Col 146 <[https://hansard.parliament.uk/Lords/2017-10-10/debates/22188EC1-6BAB-4F06-BE64-5831ABAF78E2/DataProtectionBill\(HL\)#contribution-F6C4D06C-C86F-4A40-9402-E37CCE3F7835](https://hansard.parliament.uk/Lords/2017-10-10/debates/22188EC1-6BAB-4F06-BE64-5831ABAF78E2/DataProtectionBill(HL)#contribution-F6C4D06C-C86F-4A40-9402-E37CCE3F7835)> accessed 24 November 2017.

¹⁸ pt 1, sch 1 in respect of (b), (h), (i) and (j) – each of the grounds are dealt with individually – and pt 2, sch 1 in respect of (g). Cf sch 3 to the DPA 1998.

¹⁹ Within the meaning of s 145(8) Consumer Credit Act 1974.

²⁰ art 15(1) and (3) GDPR.

²¹ cl 15(2) DP Bill.

²² These are based on those in s 12(2)(b) DPA 98.

3. Derogation Rules

Derogations are dealt with by Clause 14 which cross-refers to Schedules 2-4. These schedules list the exemptions and any conditions applying to the relevant exemption. In general, consistency with the current legal regime can be seen, as the exemptions found in the DPA 98 have been repeated in the DP Bill. This includes a number of ‘miscellaneous exemptions’ from the DPA 98, although it is not always clear where this latter group fits within the GDPR schema. It seems that a broad approach to the granting of exemptions has been adopted.²³ A couple of oddities can be noted in the text. First, the relationship between the new academic purposes definition and research purposes is not clear; should those carrying out academic research have recourse to both exemptions and when? Secondly, the journalism exception refers only to Independent Press Standards Organisation (IPSO)²⁴, in relation to press regulation, and not to the Independent Monitor for the Press CIC (IMPRESS). At the time of writing, IMPRESS is the only regulatory body recognised under the system which was set up following the Leveson Report²⁵; IPSO is not so recognised. Additionally, the Government has added some exemptions not found in the DPA. Notably, it has introduced a very broad exemption for the purposes of ‘effective immigration control’ and investigation of such matters. The provision allows data sharing between controllers (and seemingly not just public authorities) and exempts the controller from the obligations in Articles 13(1)-(3), 14(1)-(4) and 15(1)-(3) GDPR, as well as Article 5 in relation to those articles. This is in addition to any exemption in relation to crime generally. This may be

a particularly sensitive point in relation to the treatment of EU nationals post-Brexit.

The Government stated that it would exercise the derogations in Article 89(2) and (3) GDPR so that research organisations would not have to comply with a data subject’s rights to access (Article 15), rectification (Article 16), restrict further processing (Article 18) and object to processing (Article 21), but this would be limited to the circumstances where the data subject’s rights would seriously impede the researchers’ ability to complete their work and, furthermore, provided that appropriate organisational safeguards were in place to keep the data secure. Nonetheless, the safeguard provision in relation to archiving, research and statistical purposes within the context of Article 89 GDPR seems weak. It identifies just two circumstances in which Article 89(1) would not be satisfied, both of them narrowly defined – only when i) processing is carried out with respect to an individual or ii) when the individual is likely to be caused substantial damage or substantial distress. The list is, admittedly, not defined in exclusive terms but it is unclear what else would not satisfy Article 89. The absence of positive requirements is a startling one in this context.

Clause 15 empowers a Secretary of State to amend the provisions in relation to Articles 6(3), 23(1), 85(2) and 89 GDPR. Clause 15(2) specifically empowers the Secretary of State to amend or repeal the provisions relating to exemptions. There is no requirement that the effect of any such amendment or repeal is that the data subjects’ rights are safeguarded to the same or a more extensive extent. In sum, this provision could undercut the protection awarded to data subjects. While any regulations made under this provision must be made by affirmative resolution procedure, such matters do not attract the same attention or time as primary legislation. Note that in relation to matters outside the scope of EU law (effectively post-Brexit) the Secretary of State may amend the act seemingly in anyway thought fit by secondary legislation.²⁶

4. Rules on International Data Transfers

International transfers on the basis of Article 49(1)(d) GDPR are dealt with in Clause 17 DP Bill, which allows for the making of domestic regulations to allow certain data transfers from where they are ‘necessary

23 See eg, Liberty Briefing on the Data Protection Bill 2017 for Committee Stage in the House of Lords, 11 <<https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%20Briefing%20on%20the%20Data%20Protection%20Bill%202017%20Committee%20Stage%20Lords%20Oct%202017%20.pdf>> accessed 24 November 2017.

24 For further details on IPSO and IMPRESS: <<https://www.ipso.co.uk/>> and <<https://www.impress.press/contact-us/>> accessed 24 November 2017.

25 Leveson Inquiry – Report into the culture, practices and ethics of the press (29 November 2012) <<https://www.gov.uk/government/publications/leveson-inquiry-report-into-the-culture-practices-and-ethics-of-the-press>> accessed 24 November 2017.

26 cl 21 DP Bill; see comments of Lord Stevenson of Balmacara, Hansard 15 November 2017, col 2036-7 <[https://hansard.parliament.uk/Lords/2017-11-15/debates/9DC4D211-3573-4D97-82DB-92B75547B506/DataProtectionBill\(HL\)](https://hansard.parliament.uk/Lords/2017-11-15/debates/9DC4D211-3573-4D97-82DB-92B75547B506/DataProtectionBill(HL))> accessed 27 November 2017.

for important reasons of public interest'. While the resulting regulations may contain safeguards to protect against the undermining of safeguards (especially in the context of onwards transfers),²⁷ it is notable that there is no such requirement on the face of the DP Bill. Nor is the Secretary of State obliged to inform the European Commission, though notification about national provisions setting limits to the transfer of specific categories of data to a third country or an international organisation for important reasons of public interest is envisaged in Recital 112 GDPR.

5. Rules on Integrating GDPR in a post-Brexit Setting

Part 2, Chapter 3 applies to processing in the course of an activity outside the scope of European Union law²⁸ and would therefore apply post-Brexit. This is referred to as the 'applied GDPR'. By Clause 20(1), the GDPR applies, but seemingly only its articles. Whether recitals would have any ongoing interpretive status is unclear. All the provisions in relation to exceptions and clarifications permitted by the GDPR continue to apply – save as further amended. These details are set down in Schedule 6. Note that Clause 21 also grants the Secretary of State broad powers to make further modifications by statutory instrument. Additional exceptions relate to national security and defence, which specify that certain obligations and rights of data subjects (including certain protections regarding special categories of data²⁹) are not applicable in the context of national security or defence. While the DPA 98 contained exceptions for national security, the reference to 'defence purposes' is new; it is not entirely clear what might fall within its scope. The ICO makes the point that it appears to be more widely drawn than the more specific exemption in the DPA 98 of 'likely to prejudice combat effectiveness of the armed forces'.³⁰ A Minister of the Crown may issue a certificate certifying that exemption from the specified conditions is necessary for national security and any such certification 'is conclusive evidence of that fact'.³¹ The certificates are not limited in time. There is a right of appeal to the Tribunal. There seems to be no equivalent provision in relation to defence purposes.

Schedule 6 generally operates to enable the terms of the GDPR to make sense as domestic UK law. It also limits the protections awarded by the GDPR. No-

tably the extraterritorial effect of the GDPR will not apply to the applied GDPR.³² The amendments in Schedule 6 to Article 9(2) will remove the safeguards in relation to the requirement (found in current Article 9(g) and (j) GDPR) that the processing be proportionate and respect the essence of the right. The text containing those requirements is in both instances to be deleted. Article 22 is also amended to refer back to Clause 13 of the DP Bill (discussed above). Article 22(2)(b) is deleted. Clause 13 does not exactly replicate Article 22, as the reference to the 'data subject's rights and freedoms and legitimate interests' is removed. This could lead to a weakening of protection of individuals' rights.

The post-Brexit system envisages deferring to the Commission's assessment as to the adequacy of third countries' data protection regimes (under Article 45 GDPR) and specifies that a transfer must not take place if such a decision had been suspended, amended or repealed under Article 45(5) GDPR. Use of the adequacy mechanism system is envisaged to be the default, with the other mechanisms – as in the GDPR – applying only when there is no such decision. The post-Brexit system does not envisage relying on the Commission's standard data protection clauses but only those adopted by the ICO. Further, the specification of format and procedures in Article 47(3) will not have any effect.

6. The Information Commissioner and Investigations

Part 5 deals with the continuing existence³³ and powers of the Information Commissioner who will, in addition to the responsibilities under the GDPR, have responsibilities in regards to the Law Enforcement Directive.³⁴ Her powers will continue post-Brexit.

²⁷ art 46 GDPR.

²⁸ cl 19(1) DP Bill.

²⁹ cl 26 DP Bill.

³⁰ Information Commissioner's Office, 'Annex. Data Protection Bill, House of Lords Committee stage - Information Commissioner's briefing' <<https://ico.org.uk/media/about-the-ico/documents/2172658/dp-bill-lords-briefing-committee-stage-combined-annex-20171030.pdf>> accessed 4 December 2017.

³¹ cl 25(1) DP Bill.

³² cl 8, sch 6 and cl 186 DP Bill.

³³ cl 112 DP Bill.

³⁴ cl 114 DP Bill; Nb also art 13 Convention 108.

Clause 115 of the DP Bill is a new provision which implements the requirements of Article 55(3) GDPR (as well as Article 45(2) Law Enforcement Directive). In general, the powers of the supervisory authority as required by the GDPR are found in this part of the DP Bill, including the duty to develop wider international co-operation mechanisms (see Article 50 GDPR). In the light of Brexit, these mechanisms may become important. Given the expanded scope of the Information Commissioner's role, a number of concerns have been expressed about the adequacy of resources granted to her office. The Government has pointed out that 'the Bill replicates relevant provisions of the Digital Economy Act 2017, which ensures that the Information Commissioner's functions in relation to data protection continue to be funded through charges on data controllers'.³⁵ This unfortunately says nothing about the adequacy of that funding process.

Part 6 starts by providing the Information Commissioner with the powers to issue a range of notices, requesting information, requiring the controller to allow an assessment of compliance ('assessment notice')³⁶, which is a change from the DPA 98, and enforcement notices.³⁷ The Monetary Penalty Notice under the DPA will - in effect - remain (called a penalty notice) as the mechanism by which the Information Commissioner may issue administrative fines, as required by the GDPR.³⁸ Clause 148(3) contains a list of factors to be taken into consideration when deciding on whether to issue a notice and what the size of any penalty should be. The procedure in relation to the current monetary penalty regime remains the same, with the Information Commissioner being required to issue a 'notice of intent' in advance of serving a penalty. The Information Commissioner is required to publish guidance on how she proposes to

exercise her functions in relation to these three types of notice. Individuals served with a notice may appeal against it.

Part 6 also contains provisions relating to the rights of data subjects. The right to complain is clearly stated – an improvement on the position under the DPA 98. In addition to the right to complain,³⁹ data subjects will have an additional rights when they are dissatisfied with the progress (or lack of progress) of an ICO investigation. Clause 157 provides a data subject may apply to the Tribunal if the data subject believes that the ICO has not taken appropriate steps to respond to the data subject; does not provide the data subject with information on the progress of a complaint; or fails to notify its progress to the data subject. This is the Government's approach to Article 78(2) GDPR. Note that the DP Bill incorporates Article 80(1) GDPR⁴⁰ but does not provide for Article 80(2). As regards compensation as specified under Article 82, Clause 159 specifies that 'material or non-material' damage 'includes financial loss, distress and other adverse effects' – a broad, non-exhaustive list. These penalties are available even outside the scope of the GDPR. The Government stated that it intended to replicate the existing processes and safeguards applicable to civil monetary penalties under the DPA 98 to implement Article 83 GDPR.

The DP Bill retains most, but not all, existing offences under the DPA 1998. For example, the DP Bill includes the offences relating to unlawful disclosure of personal data obtained by the ICO in connection with its investigations, as well as offences relating to enforced subject access (eg where an employer asks a prospective employee to obtain personal data to which the organisation would not normally be entitled). The DP Bill extends the current offence of unlawfully obtaining personal data⁴¹ to cover unauthorised 'retention' of data.⁴² Clause 161 contains a public interest defence. Three offences in the DPA relating to the obstruction of the Information Commissioner's investigations have been consolidated into a single offence of obstruction.

The DP Bill introduces a number of new criminal offences. One such offence is that of altering, destroying or concealing information to be provided to an individual through a subject access request.⁴³ This is an extension of the offence in the FoI so that it applies to all data controllers and processors, not just public authorities. Intentionally or recklessly re-identifying individuals from anonymised or pseudo-

35 Baroness Williams of Trafford, Hansard 10 October 2017, col 214 <[https://hansard.parliament.uk/Lords/2017-10-10/debates/A0271CAB-90BC-49BD-B284-664918EE70CA/DataProtectionBill\(HL\)#contribution-D55A09C1-ADAE-4C89-9DD3-AD3856ED9861](https://hansard.parliament.uk/Lords/2017-10-10/debates/A0271CAB-90BC-49BD-B284-664918EE70CA/DataProtectionBill(HL)#contribution-D55A09C1-ADAE-4C89-9DD3-AD3856ED9861)> accessed 4 December 2017.

36 cl 140 DP Bill.

37 cl 142 DP Bill.

38 cl 148 DP Bill and sch 16.

39 cl 156 DP Bill.

40 See cls 159(2)-(3), 173 and 182.

41 s 55 DPA 98.

42 cl 161 DP Bill.

43 cl 163 DP Bill.

nymised data will also be an offence,⁴⁴ but it is subject to the same defences as the unlawful obtaining of information offence: prevention/detection of crime; authorised by law/court order; or in the public interest. This latter offence derived from the Caldicott Review of Data Security Consent and Opt-outs (in the context of health care) that was picked up in the Government's Digital Strategy. As regards the replacement for the Section 55 DPA offence, despite numerous recommendations to make this a custodial offence,⁴⁵ it remains non-custodial.

IV. Conclusion

In sum, it is noticeable that whenever there was an option available to the Government, it chose to lim-

it the rights of data subjects; the additional offences do not compensate for this. On its own, Part 2 might be sufficient for an adequacy decision, or some transitional arrangement. There remains, however, the question of law enforcement and – particularly intelligence service – access to data (both as a consequence of the DP Bill, but also the Investigatory Powers Act 2016⁴⁶). Post-Brexit and following *Schrems*, these are relevant considerations for the Commission which might be more problematic.

44 cl 162 DP Bill.

45 See eg, Leveson Inquiry (n 25).

46 Cf on this previous reports by Lorna Woods, 'United Kingdom: Draft Investigatory Powers Bill' (2016) 2(1) EDPL 103-107; 'United Kingdom: The Investigatory Powers Act 2016' (2017) 3(1) EDPL 103-105.