University of Cambridge

Briefing Paper on the Data Protection Bill

1. The purpose of this briefing paper is to summarise the key features of the UK Data Protection Bill as they affect the University's GDPR preparations.

2. The forthcoming Bill was announced in the Queen's Speech on 21 June 2017, and on 8 August 2017 the Government published a Statement of Intent regarding the Bill at the same time as announcing the results of the 'Call for Views' consultation on the GDPR derogations (to which the University responded in May 2017). Relevant documentation is available from https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law.

3. The Bill was given a first reading in the House of Lords on 13 September 2017; this formality signals the start of the Bill's passage through Parliament. A second reading, including a debate, is scheduled in the House of Lords for 10 October 2017. Once it receives Royal Assent, which is anticipated before May 2018, the legislation will be known as the Data Protection Act 2017. The draft Bill is available from https://services.parliament.uk/bills/2017-19/dataprotection.html and various Government factsheets are available from https://www.gov.uk/government/collections/data-protection-bill-2017.

4. The Bill is a long (203 pages) and complex (194 sections and 18 Schedules) document, cross-referring repeatedly to the GDPR and other legislative instruments. In summary, its purposes are:

   (a) To repeal the Data Protection Act 1998 in full (paragraph 2 of Schedule 18).

   (b) To create a comprehensive new legal framework for data protection law in the UK. This framework, of course, is supplemented automatically by the GDPR while the UK remains a member of the EU; at the point of EU exit the GDPR will be incorporated into UK law under the European Union (Withdrawal) Bill, also currently before Parliament. The purpose of transposing the GDPR into UK law is to try to achieve an early finding of data protection 'adequacy' for the UK from the EU Commission, allowing unhindered personal data flows between the UK and the EU to continue after Brexit. (One of the Government's Brexit policy papers published in August 2017 was devoted to this topic: https://www.gov.uk/government/publications/the-exchange-and-protection-of-personal-data-a-future-partnership-paper).

   (c) To enact (in Part 2) the UK's permissible Member State derogations from the GDPR (including the legal bases for processing special category personal data and exemptions from data subject rights) and to define certain terms used in the GDPR in a UK context (including 'public authority/body'). In large part, wherever possible the Bill carries forward the existing relevant provisions in the DPA 1998.

(d) To implement (in Part 3) the EU's Law Enforcement Directive that was published alongside the GDPR (see http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN and https://ico.org.uk/for-organisations/data-protection-reform/law-enforcement-directive/), which relates to the use of personal data by criminal justice agencies. (Part 2 also makes provision for the use of such personal data by data controllers which are not criminal justice agencies.)

(e) To extend (in Part 4) comparable provisions to personal data processed for national security purposes (which lies outside EU competency and so is not covered by the GDPR).

(f) To confirm (in Parts 5 and 6) the role and powers of the ICO (including with regard to fines), and to carry forward existing/create new criminal offences concerning the misuse of personal data.

5. Much of the Bill either is not relevant to the University, or will be of relevance but only in very limited operational circumstances and accordingly is not noteworthy at this stage. In broad terms, the Bill does not affect the University's GDPR preparations or the Project Plan and it confirms many of our original assumptions and (at times) aspirations. Some of the more significant points to note are as follows:

(a) The GDPR terms 'public authority' and 'public body' are defined to have the same meaning as that in the Freedom of Information Act 2000, though the Secretary of State may amend those definitions by Order. This means that, by default, UK universities (and Oxbridge Colleges) are public authorities for GDPR purposes. (Section 6.)

(b) Data processing under the GDPR legal basis that the "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" is defined as including (but is not limited to) processing that is necessary for "the exercise of a function conferred on a person by an enactment". This means that any personal data processing that is required to meet any function conferred by any UK legal instrument may be carried out under this legal basis. The Secretary of State retains the power to make further clarifications of this by Order. (Sections 7 and 15.)

(c) The age at which a child is deemed capable of giving their own consent to the processing of their personal data in the context of an online service is set at 13. (Section 8.)

(d) Provisions are made to gloss some of the legal bases for the processing of special category personal data without explicit consent. These might apply to medical data processed in some research contexts or personal data collected in connection with equalities monitoring if there is not a clear consent to such processing. Of particular relevance are: (i) that research processing meets the relevant condition in Article 9(2)(j) of the GDPR only if it is 'in the public interest'; and (ii) that the 'substantial public interest' legal basis in Article

9(2)(g) is glossed so that a data controller must create an 'appropriate policy document' explaining its reliance on that legal basis, which must meet one of a list of specific conditions (e.g. equalities monitoring or counselling). This 'policy document' requirement (essentially a statement outlining data minimisation and limited retention) is a new concept in UK data protection law and the University will need to create these where it feels it is relying on one of these conditions. (Section 9 and Parts 1-2 of Schedule 1.)

(e) Provisions are made to allow the processing of personal data about (alleged or actual) criminal convictions and offences by data controllers other than criminal justice agencies. In a University context, this might apply to staff checks, staff/student disciplinary proceedings or due diligence about prospective donations. Such processing can rely on any legal basis set out in Schedule 1. These permit processing without consent in certain circumstances, such as employment screening or crime prevention. Some (but not all) of these involve the 'policy document' requirement mentioned above, but in broad terms they replicate the conditions for the processing of such personal data that already exist under the DPA 1998. (Section 9 and Parts 1-3 of Schedule 1.)

(f) A wide range of exemptions from data subject rights (including the right to receive privacy notices and the right of subject access) are enacted. These are largely familiar from the DPA 1998 and include where the personal data are processed: for crime/taxation/judicial/legal purposes; for public protection purposes or in the exercise of regulatory functions; for management forecasting; in pursuit of negotiations; and (notably in an HE context) within exam scripts. The DPA 1998's provisions about the circumstances in which subject access requests can be refused if they involve the disclosure of personal data about other people are retained. The Secretary of State retains the power to make further exemptions by Order. (Sections 14-15, and Parts 1-4 of Schedule 2.)

(g) The existing wide-ranging exemptions from data protection law (including the principles as well as the data subject rights) in the DPA 1998 for journalism, literature and art ('the special purposes') are carried forward and extended to explicitly now include 'academic purposes'. In all cases the exemptions only apply to the extent that the processing is being carried out with a view to publication, where that publication would be in the public interest, and where the application of the GDPR's provisions would affect the special purposes. (It is worth noting that these provisions do not exempt academic activity from other UK laws such as defamation.) The Secretary of State retains the power to make further exemptions by Order. (Sections 14-15, and Part 5 of Schedule 2.)

(h) Exemptions are made from some of the data subject rights (of access, correction, restriction and objection) where personal data are processed solely for archiving or scientific/historical research purposes, but only when that research does not lead to measures or decisions about an individual and where it is not likely to cause them substantial damage or distress. It is worth

noting that (as under the DPA 1998) there is no exemption from the core data protection principles or from the requirement to supply privacy notices when personal data are processed in scientific/historical research contexts. The Secretary of State retains the power to make further exemptions by Order. (Sections 14-15 and 18, and Part 6 of Schedule 2.)

(i) Provision is made for the Secretary of State to make Orders permitting the transfer of personal data outside the EEA for reasons of substantial public interest in the absence of any alternative adequacy mechanism. (Section 17.)

(j) Provision is made to extend data protection law to manual unstructured personal data processed by public authorities – such information is not caught by the GDPR definition of 'personal data'. However, the majority of the GDPR (including the principles other than of accuracy) is then dis-applied. The rationale for this is: (a) to ensure that such personal data may be requested under subject access rights; and (b) to ensure that such personal data are subject to exemptions from the Freedom of Information Act 2000. The drafting is complex but in short is intended to replicate the current situation under the DPA 1998. (Sections 19 and 22.)

(k) The ICO is granted the same status and similar powers (including of information gathering, audit, assessment, enforcement, entry and inspection, and the charging of fees to data controllers) as those under the DPA 1998. The ICO is asked to issue statutory direct marketing and data sharing Codes of Practice, but a failure to adhere to these is not itself an offence. Its fining powers are capped in Euros as in the GDPR. (Sections 113, 119-120, 132 and 150.)

(l) Various personal criminal offences are newly created or carried forward from the DPA 1998. These include: refusing to supply the ICO with information; unlawfully obtaining personal data; recklessly re-identifying de-identified personal data; altering or deleting personal data to prevent disclosure once it has been requested under subject access rights; enforcing subject access; and refusing to supply the ICO with information or blocking the ICO's entry and inspection. Company directors are personally liable if an offence is committed with their consent or connivance, or as a result of their neglect. (Sections 139, 161-163, 171, Schedule 15, section 177.)

6. It is worth stressing that the Bill is likely to be subject to amendment as it progresses through Parliament.

Dr James Knapton
Information Compliance Officer
Registrary's Office
28 September 2017