UNIVERSITY OF CAMBRIDGE

COUNCIL

BRIEFING PAPER ON THE GENERAL DATA PROTECTION REGULATION

Purpose

This briefing paper is designed to give members of the Council a high-level summary of the General Data Protection Regulation (*GDPR*), its impact upon the University, and the actions that have been taken and will be taken to address it.

> Updates 29 August 2017 and 3 October 2017
> Shaded text boxes have been inserted at relevant points within this document to provide updates on matters of legislative interpretation and/or significant changes of policy since it was first published in April 2017. Please note that these update boxes do not list the various practical preparations that have been undertaken or completed to date.

Executive summary

Key facts about the GDPR

- The GDPR will apply from 25 May 2018 and will replace the Data Protection Act 1998 (*DPA*).
- The GDPR sets out a more prescriptive and punitive regulatory framework for organisations to follow when processing personal data (information about living identifiable individuals). Nevertheless it is open to different interpretations because it is a 'principles-based law' (in other words, compliance is assessed primarily by adherence to a set of data protection principles).
- In order to process the personal data of different types of data subject, a data controller must determine in advance the relevant legal basis for doing so from a prescribed list and must supply the data subject with detailed information about how their personal data will be used.
- Data subjects have strengthened rights under the GDPR.
- Data controllers must implement a detailed set of accountability measures to demonstrate their compliance with the GDPR.
- Regulatory fines for non-compliance with the GDPR are subject to an upper limit of €20m or 4% of turnover (whichever is higher).

Key implications of the GDPR for the University

- The University must reconsider its legal basis for processing the personal data of different types of data subject.
- The University must realign its engagement mechanisms with its data subjects, and the information it provides to them, with GDPR standards.
- The University needs to be able to respond adequately to the strengthened rights of data subjects.
- The University must implement the new accountability measures to demonstrate its compliance with the GDPR. It needs to embed a culture of data protection awareness and revise its existing relevant policies, procedures, guidelines and training to GDPR standards.
- The University's preparations for the GDPR are being overseen by the GDPR Data Protection Working Group, which is coordinating its activities wherever possible with those of other bodies pursuing related programmes of work.

Key external uncertainties surrounding the GDPR

- The UK definitions of a 'public authority' and its 'tasks' for GDPR purposes are unclear. Different legal bases for the processing of personal data are available depending on these definitions. Further, 'public authorities' are subject to some additional accountability requirements.
- The content of the UK's permitted subsidiary national legislation under the GDPR, some of which is particularly relevant to the HE sector (e.g. on personal data and research), is unknown.
- The impact of Brexit on the long-term operation and regulation of the GDPR in the UK is unknown.

Update 29 August 2017
Some of these uncertainties are becoming clearer; see the update boxes at paragraphs 1, 4 and 17 below.

Update 3 October 2017
These uncertainties largely are now resolved; see the update boxes at paragraphs 1, 4 and 17 below.

Contents

Briefing paper

The GDPR and data protection law

1. The GDPR, following over four years of negotiations across EU institutions, was published in the Official Journal of the European Union on 4 May 2016.[1] It came into force on 25 May 2016 and will apply from 25 May 2018. As a European Regulation, it applies in full in all Member States without national legislation to implement it, although governments are permitted to introduce subsidiary national legislation to create limited derogations from, and supplements to, some of its provisions. It is designed to harmonise and strengthen the standard of data protection law across the EU; in so doing, it repeals the European Directive that led, in the UK, to the DPA.[2] After a hiatus caused by the EU referendum result, the UK Government in late October 2016 confirmed that, as the UK will remain an EU Member State in May 2018, the GDPR necessarily will apply in this country and much of the DPA will be repealed. It has further indicated that the GDPR (or a national version of it) is likely to be retained beyond the country's formal exit from the EU so as to enable the UK Government to apply to the EU Commission for 'adequacy' status, meaning that UK-EU personal data transfers may continue without additional safeguards. The UK Government published its 'call for views' about the permitted subsidiary national legislation on 12 April 2017 for responses by 10 May 2017.[3] This consultation document neither indicates current Government thinking nor outlines the timetable for the subsequent enactment of this legislation.

   Update 29 August 2017
   Following the 'call for views' exercise, the Government issued a 'statement of intent' announcing its plans to implement its permitted subsidiary national legislation through a Data Protection Bill, to be introduced in autumn 2017, which will also embed the provisions of the GDPR into UK law for the post-Brexit era (see https://www.gov.uk/government/consultations/general-data-protection-regulation-call-for-views).

   Update 3 October 2017
   The Data Protection Bill had its first reading in the House of Lords on 13 September 2017 (see https://www.gov.uk/government/collections/data-protection-bill-2017).

2. The GDPR, like the DPA, sets out rules and standards for the processing (collection, use, storage, sharing and destruction) of the personal data of data subjects (information relating to living identifiable individuals) by data controllers

[1] The text of the GDPR is published at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. An overview has been published by the Information Commissioner's Office at https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/. Numerous similar guides have been produced by law firms and others.
[2] The text of the DPA is published at http://www.legislation.gov.uk/ukpga/1998/29.
[3] The call for views is published at https://www.gov.uk/government/consultations/general-data-protection-regulation-call-for-views.

(organisations).[4] It does not apply to information about the deceased, to anonymous information or to personal data rendered anonymous in such a manner that the data subject is no longer identifiable. It also does not apply to information about individuals that is processed solely by non-electronic means in an unstructured way. The University of Cambridge is a single data controller, and each of the 31 Colleges is a separate data controller. Cambridge Assessment and Cambridge University Press, although formally departments of the University, have been registered as separate data controllers under the DPA; they will continue to act independently in data protection matters under the GDPR but with a greater degree of cooperation and coordination with the University.

Update 29 August 2017
While the University, Cambridge Assessment and Cambridge University Press will continue to act semi-independently on data protection matters at an operational level under the GDPR, it is now considered that these three parts of the University Group should work together much more closely on data protection strategy and policy.

3. The GDPR's rules and standards are based around the familiar concepts of data protection principles and data subject rights. As a whole, it is substantially more prescriptive than the DPA in describing how data controllers should implement the principles and respond to data subjects exercising their rights. In addition, it places a new emphasis on a data controller's ability to demonstrate its compliance with the law. Nonetheless, the GDPR remains a principles-based law and consequently compliance with its provisions will necessitate numerous risk-based interpretations of indistinct terms such as 'fair', 'reasonable', 'appropriate', 'proportionate', 'adequate', 'necessary' or 'legitimate'.

4. At times, the GDPR sets different rules and standards for data controllers that are public authorities as opposed to those that are not. Neither the GDPR nor wider EU law defines public authorities. The GDPR will be regulated in the UK by the Information Commissioner's Office (*ICO*), which is also the regulator of the Freedom of Information Act 2000 (*FOIA*). The University and each College are classed with public authorities for the purposes of the FOIA and, unless subsidiary national legislation is introduced to determine the point one way or another, it appears likely that the ICO will view HE sector institutions as public authorities for the GDPR as well. Such a classification does not naturally accord with the notion of a public authority in the GDPR – essentially an agent of the state carrying out exclusively public functions under statute – and for this reason the University has been seeking some clarity over the definition, whether legislative or otherwise, and has been lobbying for the exclusion of the HE sector from it.

Update 29 August 2017
The Government's 'statement of intent' has indicated that the GDPR definition of a 'public authority' will be taken from the FOIA.

Update 3 October 2017

[4] The full definitions of these terms are given in Article 4 of the GDPR.

This definition of a 'public authority' is confirmed in the Data Protection Bill.

The data protection principles and the lawfulness of personal data processing

5. The data protection principles as set out in Schedule 1 of the DPA and Article 5 of the GDPR can be summarised as follows:

DPA Schedule 1 Personal data shall be:	GDPR Article 5 Personal data shall be:
1: processed fairly and lawfully	1a: processed fairly, lawfully and transparently
2: processed only for specified and lawful purposes	1b: processed only for specified, explicit and legitimate purposes
3: adequate, relevant and not excessive	1c: adequate, relevant and limited
4: accurate	1d: accurate and rectified if inaccurate
5: not kept for longer than necessary	1e: not kept for longer than necessary
6: processed in accordance with subjects' rights	Not a principle but covered elsewhere in GDPR (Chapter III)
7: processed securely	1f: processed securely
8: not transferred outside the EEA without adequate protection	Not a principle but covered elsewhere in GDPR (Chapter V)
Not covered in DPA	2: data controller must be able to demonstrate compliance with 1a-1f

Essentially, the core principles remain the same. The changes reinforce the notions of transparency and accountability.

6. Both the DPA and the GDPR state that a data controller may only process personal data if there is a legal basis for doing so. Article 6 of the GDPR sets out the available bases, which can be summarised as follows:

(i) Article 6(1)(a): with the consent of the data subject.[5] Article 7 further states that consent should be clear, affirmative, easily withdrawable, retrospectively demonstrable and kept separate from the conclusion of a contract or the receipt of a service. It should not be enforced or offered where there is no genuine choice or an imbalance in the relationship between data controller and data subject. Article 8 further states that where the personal data of a

[5] The ICO's first and, at the time of writing, only piece of specific GDPR guidance to date, albeit only in draft form and of a non-statutory nature, is on the topic of consent: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf.

child are processed in an online environment, parental consents must be collected.[6]

(ii) Article 6(1)(b): the processing is necessary to operate a contractual relationship with a data subject, or to prepare for such a contractual relationship at the initiation of the data subject.

(iii) Article 6(1)(c): the processing is necessary to comply with a legal obligation.

(iv) Article 6(1)(d): the processing is necessary to protect the vital (life or death) interests of the data subject.

(v) Article 6(1)(e): where allowed for *under law*, 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'. Member States are permitted to clarify or expand upon this legal basis in subsidiary national legislation. Neither 'a task carried out in the public interest' nor 'the exercise of official authority' are defined in the GDPR and accordingly the extent to which this legal basis can relied upon by HE sector institutions is unknown. It is anticipated that processing under this legal basis will relate primarily to personal data processed in pursuit of the core statutory functions of an organisation.

(vi) Article 6(1)(f): the processing is necessary to pursue the legitimate interests of the data controller, where those are not overridden by the data subject's own interests. This legal basis is not available 'to processing carried out by public authorities in the performance of their tasks'. Neither 'public authorities' nor their 'tasks' are defined in the GDPR. This, coupled with the absence of either a certain definition in UK law or an authoritative GDPR-specific announcement by the Government or the ICO on this point, is a significant concern because the extent to which this legal basis can relied upon by HE sector institutions is unknown. It is anticipated that processing under this legal basis by public authorities will relate primarily to personal data processed in pursuit of the ancillary (i.e. non-core) functions of an organisation.

Update 29 August 2017
The Government's 'statement of intent' has indicated that the GDPR definition of a 'public authority' will be taken from the FOIA. The ICO's public pronouncements on the legal bases for processing nonetheless repeatedly have stressed the view that the legitimate interests legal basis will remain available to public authorities whenever they are not pursuing their core functions.

Update 3 October 2017
This definition of a 'public authority' is confirmed in the Data Protection Bill.

7. Article 9 of the GDPR sets out the available legal bases for the processing of special category (sensitive) personal data, which broadly means personal data relating to a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual life/orientation, as well as their

[6] The GDPR defines a child in this context as someone under 16 years of age, but allows Member States to introduce subsidiary national legislation to reduce this to under 13.

genetic or biometric data.[7] Some of the most relevant of these can be summarised as follows; Member States are permitted to add others in subsidiary national legislation:

(i) Article 9(2)(a): with the explicit consent of the data subject.
(ii) Articles 9(2)(b) and 9(2)(g): the processing is necessary to comply with an obligation under employment or social protection law, or under another law where the public interest necessitates the processing.
(iii) Article 9(2)(c): the processing is necessary to protect the vital (life or death) interests of the data subject.
(iv) Articles 9(2)(h) and 9(2)(i): the processing is necessary for health, occupational health or public health purposes.
(v) Article 9(2)(j): the processing is necessary for research purposes under certain safeguards.

8. While it was always obligatory to have a valid legal basis to process personal data under the DPA, the legal basis takes on additional significance under the GDPR. This is because it must be stated up-front to the data subjects and because it affects the ways in which those subjects are allowed to exercise their rights. For some of the standard types of data subject whose personal data are processed by the University, the likely legal bases under the GDPR can be simplified and summarised as follows:

(i) The personal data of applicants may be processed under the pre-contract basis (Article 6(1)(b)).
(ii) The personal data of students may be processed in the main under the contract basis (Article 6(1)(b)). This does not mean that students must be issued with new standalone contracts, as existing documents sent to offer-holders suffice to act as the contract between the University and the future student in this context. Supplementary consents or explicit consents may need to be sought for the *non-necessary* processing respectively of standard personal data (e.g. appearance in publicly-available class-lists) or special category personal data (e.g. student engagements with certain welfare services or processes) (Articles 6(1)(a) and 9(2)(a)).
(iii) The personal data of alumni and supporters may be processed under the consent basis to the extent not permissible under the legitimate interests basis (Articles 6(1)(a) and 6(1)(f)).[8]

---

[7] Personal data concerning alleged or actual criminal offences, which constitute sensitive personal data under the DPA, are not classed as special category personal data under the GDPR. The processing of such personal data essentially must be mandated by EU or Member State law, including the European Directive on crime-related personal data processed by 'competent authorities' that was published alongside the GDPR and needs to be implemented in UK law by 6 May 2018. The Directive is published at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN.

[8] This is on the assumption that, whether or not HE sector institutions are classed as public authorities for GDPR purposes, the processing of alumni and supporter personal data is not a statutory 'task' of a university or college and accordingly the legitimate interests legal basis remains available. Recent enforcement action by the ICO under the DPA against certain charities with regard to their fundraising practices has suggested that certain standard practices (notably the use of publicly available

(iv) The personal data of staff may be processed under the contract basis (Article 6(1)(b)) and their relevant special category personal data may be processed under the occupational health basis (Article 9(2)(h)). Supplementary explicit consents may need to be sought for the *non-necessary* processing of their other special category personal data (e.g. staff engagements with certain welfare services or processes) (Article 9(2)(a)).

(v) The personal data of research subjects may be processed under the consent basis or the public interest task basis (Articles 6(1)(a) and 6(1)(e)), and their special category personal data may be processed under the explicit consent basis or the research basis (Articles 9(2)(a) and 9(2)(j)). It should be stressed in this regard, notwithstanding the focus in research ethics on processes to gain informed consent from participants, that consent is *not* the only legal basis under which personal data (or special category personal data) can be processed for research purposes, whether for secondary re-use or otherwise.

(vi) For all categories of data subject, there will inevitably be occasions where the processing is necessary due to a legal obligation (Articles 6(1)(c), 9(2)(b) and 9(2)(g)) or to protect the data subject's vital interests (Articles 6(1)(d) and 9(2)(c)).

9. The above list largely replicates the legal bases used at present under the DPA, though the University currently seeks some blanket consents (e.g. in different ways from applicants, students and staff) that, given the lack of genuine choice, would be inappropriate under the GDPR and need to be discontinued. The most fundamental change relates to the personal data of alumni and supporters where it appears likely that consents will be required in order to process such personal data if the University is to continue to do so for the current wide variety of purposes; it is envisaged that a coordinated GDPR consent collection exercise will be launched by the University and Colleges in the near future.[9] It nonetheless remains possible, depending on how subsidiary national legislation and further ICO guidance define and/or interpret these aspects of the GDPR, that HE sector institutions may be able to rely more heavily on the legal bases of public interest task (Article 6(1)(e)) or legitimate interests (Article 6(1)(f)) than is envisaged at present.

---

information), in the ICO's opinion, can be inherently unfair in the absence of the data subject's consent, regardless of whether or not any alternative bases appear to be available to render the processing lawful. The implications of the GDPR for alumni relations and fundraising across the Collegiate University are under consideration both at the GDPR Data Protection Working Group (see paragraphs 19-21) and at the Joint Committee on Development's ad-hoc Working Group on Fundraising-related Regulations.

[9] Such an exercise would encompass the collection not only of consents from alumni and supporters under the GDPR for personal data processing but also of consents for direct email and phone marketing which are future-proofed to meet the standards of the forthcoming ePrivacy Regulation (which will replace the Privacy and Electronic Communications Regulations 2003, as amended). The Regulation was published in draft form by the European Commission in January 2017 and is therefore subject to negotiation and agreement across EU institutions, but it is ambitiously scheduled to apply on 25 May 2018 alongside the GDPR. The text of the draft ePrivacy Regulation is published at https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications. The ICO has published a blog on the topic at https://iconewsblog.wordpress.com/2017/04/05/eprivacy-reform-pecr-under-review/.

Update 29 August 2017
It is now considered that the personal data of alumni and supporters may be processed under a combination of the public interest task and legitimate interests bases, and that consents are not necessary. This position reflects both public pronouncements by, and private discussions with, the ICO.

Data protection statements

10. Regardless of the legal basis or bases being relied upon, Articles 13-14 of the GDPR set out prescriptive new requirements about the content of data protection statements (also known variously as privacy notices/statements, data protection notices, privacy policies, and so on). These are statements that must be given to data subjects about how their personal data will be used by the data controller. Under the GDPR, these: must be transparently worded and accessible; must be given at the point of data collection or normally within one month if the personal data are not directly collected; and must cover numerous topics, including the legal basis relied upon for the processing, indicative retention periods, proposed personal data sharing, and the existence of the various data subject rights.

11. Given the wide variety of data protection statements currently used in multiple ways across the University for all types of data subject (including those given to research subjects or members of the public simply visiting University websites), this rewriting exercise represents a significant challenge. In particular, the data protection statements given to all students at various points in the standard cycle (application, offer, matriculation, registration and graduation) will need to be amended and presented in a more consistent way. In addition, it will be important to adhere to any retention periods included in these statements and so the current guidance on records management and retention will need to be amended and formalised.

Data subject rights

12. Data subjects are granted an extensive range of new or enhanced rights under Articles 15-22 of the GDPR. Unless a right is exercised in a 'manifestly unfounded' or 'excessive' way, a data controller must respond within one month and cannot charge a fee. The rights can be summarised as follows:

(i) The right of access to personal data. Such requests attract a statutory fee of £10 under the DPA; the removal of this fee, however nominal, is expected to lead to a rise in the number of requests.
(ii) The right to have inaccurate personal data rectified. Copies of the corrections must normally be sent to any third parties to whom the personal data in question have been disclosed.
(iii) The right to have personal data erased (right to be forgotten).
(iv) The right to restrict the processing of personal data pending verification or correction.
(v) The right to receive copies of certain personal data in a machine-readable and commonly-used format (right to data portability).

(vi) The right to object: to processing (including profiling) under the public interest task or legitimate interests legal bases; to direct marketing; and to processing for research purposes where that research is not in the public interest.

(vii) The right not to be subject to a decision based solely on automated decision-making.

All of the rights are qualified to some degree: certain types of personal data processing are exempt from some of the rights (for example, processing for archival, statistical or research purposes broadly is exempt from the right to erasure) and Member States are permitted to introduce subsidiary national legislation to add further exemptions from the rights in various broad areas. (On a minor matter, these broad areas do not include those to do with examinations, and so it is likely that examination scripts – which currently are exempt from subject access – in future will need to be disclosed to students on request.) Nevertheless, new procedures will need to be written to enable these rights to be managed and major IT systems are being assessed to ensure that they are technically capable of fulfilling them if exercised.

Accountability: roles and responsibilities

13. Articles 24-39 of the GDPR impose a long list of responsibilities on data controllers in pursuance of their general accountability obligation. Many of these already are regarded as best practice under the DPA but now are codified as a legal requirement. All of them require either changes to the University's current policies and processes or the creation of new ones. These responsibilities can be summarised as follows:

(i) There is an organisational requirement to promote measures designed to minimise personal data use (such as pseudonymisation) and to embed data protection considerations at the start of new projects or initiatives ('data protection by design and by default'). This is a wide-ranging requirement, and guidance will be required in areas as diverse as academic research projects and IT procurement procedures.

(ii) There are new rules on the contents of the agreements that must be in place between joint data controllers. Revised data sharing agreements or protocols will be required between the University and the Colleges.

(iii) There are more detailed rules on the contents of the agreements that must be in place between data controllers and their data processors. Revised data sharing agreements or contractual clauses will be required between the University and its numerous service providers that use the personal data it holds.

(iv) There is a new requirement to maintain a register of all personal data processed across the University. This must include: the personal data categories involved in any specific processing activity; the types of recipients; whether transfers outside the EEA will happen (and, if so, how adequate safeguards will be maintained); indicative retention periods; and a general description of the relevant security measures. An information asset register is being created and populated to fulfil this requirement which replaces the current light-touch ICO registration system.

(v) There are newly prescriptive information security requirements (such as encryption and regular testing) in order to ensure the confidentiality, integrity, availability and resilience of systems and services processing personal data. In some ways these requirements simply enforce activities that are already carried out, but the accountability requirement means that the University will need to be able to demonstrate – by way of relevant policies and documentation – that it is paying due regard to this aspect of the GDPR.[10]

(vi) Certain types of personal data breach must be notified to the ICO within 72 hours, and to the affected individuals without undue delay, and records must be maintained of all personal data breaches. The University's breach reporting procedures will need to be amended and methods found for their acceleration.

(vii) Data Protection Impact Assessments are prescribed for certain types of high risk processing, in particular with regard to processing operations involving large quantities of special category personal data or the profiling of a large number of data subjects.[11] These will need to be designed for new administrative processes, new IT systems and (potentially) embedded into existing ethical review processes for some academic research projects.

(viii) All public authorities, and certain other data controllers, are required to appoint a Data Protection Officer (*DPO*), who is described as a senior role-holder with independence and expertise in fulfilment of their statutory tasks. The DPO must not receive any management instructions in pursuance of their tasks under the GDPR, must be protected from dismissal in their performance of those tasks, and must directly report to the highest management level of the organisation. The best way in which to fulfil this role at the University remains under consideration.

Update 29 August 2017
It is now considered likely that a single role of DPO will be created to cover the University Group.

14. In support of all of the above, a new overarching data protection policy, an enhanced data protection training programme and substantially revised and augmented guidance materials will be required. The revisions to training and guidance materials are not limited to those issued under a data protection banner but expand to encompass guidance for, *inter alia*, academic researchers (both with regards to engaging with human participants and research data management), alumni relations and development staff, IT staff with security responsibilities, and all those involved in implementing various aspects of student or staff policy. All of these materials will need to be consistent and easy for staff and others to access and understand. There will also be a significant number of 'consequential' amendments to existing tangential processes and procedures that involve the processing of personal data.

---

[10] There are overlaps between some of the work required in preparation for the GDPR and that being progressed as part of the University's cyber security programme overseen by the Information Security Sub-Committee of the Information Services Committee. Both the work and associated communications to staff are being coordinated wherever possible.

[11] The ICO has published a discussion paper on the GDPR and profiling: https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf.

15. The GDPR establishes and promotes the concepts of 'codes of conduct' and 'certification' schemes by which data controllers can demonstrate their compliance. It is not anticipated that any such codes or certifications will be launched for the HE sector in advance of May 2018 (or possibly beyond).

16. Like the DPA, the GDPR in Articles 44-50 sets out detailed rules under which personal data may and may not be transferred outside the European Economic Area (including transferred by way of upload to a website or cloud service that is not hosted within the EEA). The changes in these parts of the GDPR should not substantively impact upon the University, and in any event will apply in a totally different way when the UK itself is no longer an EU Member State.

Specific derogations: freedom of expression and research

17. As well as the derogations that Member States are permitted to introduce through subsidiary national legislation as signalled at various points above, some Articles towards the end of the GDPR allow Member States to introduce further legislation to govern personal data processing in certain broad areas. Of particular relevance to the University are the provisions that may be made for processing in pursuit of journalism and freedom of expression (including academic expression),[12] for processing for research purposes, and for processing for employment purposes. In all instances, these provisions allow governments to reconcile the principles of the GDPR with human rights law and existing national legislation. While the form and content of any such legislation currently is unknown, it is notable that academic research is relatively protected already within the GDPR;[13] it is hoped that the scope to introduce still further exemptions should allow most research projects to continue without undue adverse consequences.

Update 29 August 2017
The Government's 'statement of intent' has indicated that the research and freedom of expression exemptions will be implemented widely and, insofar as possible, will be aligned with comparable exemptions in the DPA.

Update 3 October 2017
These exemptions are set out in the Data Protection Bill. The exemption for processing for 'academic purposes' is very widely construed, effectively dis-

[12] The wording of this Article is designed to give certain academics, largely in the social sciences, the same freedoms from data protection law as those already granted under the DPA to non-academic journalists, commentators or historians conducting investigative research for literary or journalistic publication.

[13] Under both the DPA and the GDPR, personal data may be processed for research purposes even if those are not obviously compatible with the original purpose for which the data were collected, and such data may be retained indefinitely. There is an exemption from the requirement to supply data protection statements for research purposes where this would be impossible or would involve disproportionate effort (e.g. in the secondary re-use of existing datasets). The GDPR also permits consents for research purposes to be collected in relation to general areas of scientific research as well as specific research projects.

applying the principles, legal bases and rights (including the right to receive data protection statements) in their entirety. Another exemption, for 'scientific or historical research purposes' is more limited in scope and builds upon the specific exemptions already embedded within the GDPR, meaning that some of the principles and some of the rights are dis-applied, but not the legal bases or the right to receive data protection statements. In both cases the general accountability requirements remain in place. The ways in which these exemptions work together are likely to be complex.

Penalties

18. As well as giving an individual data subject the right to take action through the courts to seek compensation for any breach by a data controller, the GDPR grants the ICO and other national regulators the power to levy administrative fines for breaches. The current maximum fine under the DPA is £500,000; under the GDPR this is raised to €20m or 4% of turnover (whichever is higher) for infringements broadly to do with the principles, lawfulness, consent and data subject rights, and €10m or 2% of turnover (whichever is higher) for infringements broadly to do with security breaches and the various accountability and record-keeping requirements.[14] Member States can determine the extent to which administrative fines should apply to public authorities. The GDPR creates new pan-European mechanisms and organisations to harmonise fines across EU Member States. The changes to this regulatory environment after the UK has left the EU are unknown.

GDPR Data Protection Working Group

19. In summer 2016, the senior Officers of the UAS authorised the establishment of a GDPR Data Protection Working Group to work on and oversee the University's preparations for the GDPR. The Group is Chaired by the Acting Registrary and has members from the Registrary's Office, the Legal Services Office, the Student Registry, the Cambridge Admissions Office, Educational and Student Policy, University Information Services, the Development and Alumni Relations office, the Research Office, the Human Resources Division, the University Library, and the Office of Intercollegiate Services. Representatives from Cambridge Assessment and Cambridge University Press also attend. As the Group's work is now moving from a planning to an operational phase, it plans to augment its membership to include a School Secretary, with the aim of ensuring that the wider University community's interests and concerns are embedded throughout the remainder of the preparations.

Update 29 August 2017
The Working Group's membership was supplemented by two representative Departmental Administrators instead of a single School Secretary.

20. The Group's terms of reference are:

[14] Fines based on percentage of turnover relate to 'undertakings'; it is presumed that the University will fall within this definition and accordingly the upper limit of fines, given its annual turnover, would be significantly in excess of €20m.

To develop, scrutinise and approve the necessary changes to the University's policies, procedures, guidelines and training in time for the implementation of the EU's General Data Protection Regulation. Where formal Committee oversight is required for any particular change, to develop, scrutinise and recommend the necessary change to the relevant Committee.

21. The Group has formulated and approved a detailed Project Plan by which its different members are allocated as the Lead on different aspects of the preparations, whether these are the work required in relation to specific categories of data subject (applicants, students, alumni/supporters, staff, research subjects, members of the public, and so on), or the work required in creating or amending the overarching policies, procedures and processes needed to demonstrate the University's accountability. Wherever possible, the changes required for the GDPR are being implemented proportionately and are being embedded within existing policies and procedures rather than through the creation of standalone new ones; activities are being coordinated wherever possible with those of other bodies pursuing related programmes of work, such as the Joint Committee on Development's ad-hoc Working Group on Fundraising-related Regulations and the Information Security Sub-Committee. The deadlines in the Project Plan take into account the changes that will be necessary at specific points in the academic cycle where required. As well as changes to central processes, the Group is charged with the creation and dissemination of communications and guidance to University Institutions for them to plan for and implement any amendments to their local practices. While a number of individual briefings and presentations have taken place to date, a widespread communications exercise will be launched shortly.

Update 29 August 2017
Various communications activities have been undertaken and will continue (see, for example, http://www.staff.admin.cam.ac.uk/general-news/changes-to-data-protection-law). The dedicated webpage at https://www.information-compliance.admin.cam.ac.uk/data-protection/general-data-protection-regulation will always contain up-to-date information.

Conclusion

22. The Council is asked to note and comment upon this briefing paper.

Dr James Knapton
Information Compliance Officer
Registrary's Office
18 April 2017