THE UNIVERSITY OF LEEDS

General Data Protection Regulations update

1. The central aim of the GDPR, which come into force on 25 May 2018 and which will supersede the Data Protection Act 1998 (DPA), is to harmonise data protection laws throughout the EU; particularly for reasons of trade the regulations will continue to apply to the UK after Brexit.

2. The introduction of the GDPR will tighten the regulatory regime covering data protection, but has been described as more evolutionary than revolutionary: to a large extent, the new regulations crystallise what should be good practice anyway.

3. In essence, the GDPR will regulate the processing of personal data. They define 'personal data' as 'any information relating to an identified or identifiable natural person'. As with the DPA, some categories of data are classified under the GDPR as 'special'[1], and the grounds on which special categories of data may be processed are limited.

4. To help protect the security of personal data, the GDPR place a greater emphasis than does the DPA upon the practice of anonymising data wherever possible, and as a fall-back upon the pseudonymisation of data.

5. There remains a general expectation that anybody processing personal data should be asking three critical questions:

    - why do we need to collect or keep these data?
    - are all of these data really needed for that purpose?
    - and for how long do we need to keep them?

Main changes

6. The main changes introduced by the GDPR are summarised below.

More data caught

7. More personal data will be covered by the legislation; in particular, the bar has been lowered for determining when a natural personal is 'identifiable' from data; and genetic data and biometric data have been added to the list of special data (see footnote).

Collection and consent to process data

8. It is already a precept in data protection legislation that, when organisations collect data, they need to explain for what purposes the data will be processed. This precept remains under the GDPR but there will be a requirement to give individuals further and better information about the uses to which their data will be put. There will similarly be a requirement that, where consent is required, it is obtained in unambiguous language. The University will therefore need to review information notices (notices that explain what and how data are to be processed) and template consent forms.

[1] Special data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or TU membership, and the processing of genetic or biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation.

Data processors obligations

9. When the University is processing data for others (for example as part of a research consortium), it will no longer be able to pass liability back to those who have asked it to do the processing. We already have standard processing agreements, but some renegotiation may be needed with other interested parties.

Transparency

10. The University will have to introduce and maintain a register of all of its processing activities so those activities can be properly monitored for compliance. We will need to undertake an audit identifying what data are being processed, for what purposes they are being processed, with whom data are being shared, and any planned retention of personal data.

Data protection by design

11. The University must be able to show that it has designed into its processes protection for personal data, which in practice is likely to require:

    - Use of anonymous personal data where possible, and otherwise use of pseudonymisation techniques.
    - Technical IT protections (especially compulsory use of encryption).
    - Compulsory staff training.
    - Auditing of IT systems.
    - Rigorous enforcement of 'data minimisation' (taking only what data are actually needed and retaining them only as long as actually necessary, which will require adherence to agreed retention schedules).

12. For 'high risk' processing, the University will need to conduct privacy impact assessments to make sure there are the necessary controls in place. For example an assessment will be required where there is a research project involving a considerable amount of, or highly sensitive, personal data.

Enhanced individual rights

13. Individuals will have enhanced subject access rights under which they can demand a copy of their personal data, now to be without charge and to be provided within 'one month' as opposed to the current 40 days.

14. The GDPR affords individuals the 'right to be forgotten' (the right to have your data destroyed) and the 'right of portability' (the right to receive personal data in a common portable form – for example, a disk or memory stick). These rights are not absolute. In particular, the University will wish to argue that certain sets of data should be held for either indefinite or lengthy periods of time – for example, basic student transcript information and information required to be retained for regulatory or tax purposes.

15. Individuals will sometimes have the right to object to so called automated decision making and profiling.

Accountability

16. The GDPR requires the appointment of a data protection officer (DPO) whose responsibility is to provide advice and monitor compliance with GDPR. Currently, the University's Legal Adviser, Adrian Slater, is the 'data controller' for the University, reporting in this capacity through to the University Secretary. In the first instance at least, the expectation is that the Legal Adviser will serve as the DPO.

Reporting breaches

17. Under the GDPR, the University must have a proper system for recording data breaches and for reporting certain breaches to the Information Commissioner's Office within 72 hours.

Litigation and penalties

18. The GDPR will make it easier to claim compensation for harm caused by a breach of the law. For example someone may bring a claim where as a result of a data breach their data was compromised and they suffered a fraud.

19. Maximum fines will be increased under the GDPR to the higher of €20 million or 4 per cent of turnover.

Research

20. On balance, subject to researchers having to make more effort to anonymise data where possible, to assess risk and to take appropriate measures to ensure the data is held safely, GDPR offers some potential benefits for research. For example, a researcher will be able to process even sensitive data for research purposes, even if the research was not the purpose for the initial data collection.

Compliance

21. The University's Information Protection Group (IPG) has approved a working plan to ensure compliance with the GDPR. Implementation of the plan will be overseen via the IPG, with reports to UEG at appropriate intervals. In general, GDPR compliance will be effected through implementation of measures already in train to strengthen IT security, with a few changes of practice being required in the University, consideration is also being given to the implications for fund-raising practice.

    More information can be found on the ICO website:
    https://ico.org.uk/for-organisations/data-protection-bill/

    and on the Pinsent Masons website:
    https://www.pinsentmasons.com/en/expertise/sectors/advanced-manufacturing--technology/eu-general-data-protection-regulation/

The Secretariat
October 2017