General Data Protection Regulation: academic research

James Knapton, Information Compliance Officer, Registry’s Office
What is the GDPR?

- EU General Data Protection Regulation has applied *in full* since 25 May 2018
- Supplemented in UK by new Data Protection Act 2018 that adds additional rules and exemptions
- UK Data Protection Act 1998 was repealed on same date
- Sets standards for handling (‘processing’) of information (‘personal data’) about living identifiable individuals (‘data subjects’) by organisations (‘data controllers’)
  - Data protection principles and data subject rights
  - Certain types of activity exempt from certain aspects of the standards
- More prescriptive and punitive than DPA 1998: Information Commissioner’s Office (ICO) fines up to €20m instead of £500k
Principles

• Personal data shall be:

  ➢ Processed fairly, lawfully and transparently – and only if a valid ‘legal basis’ exists
  ➢ Processed only for specified, explicit and legitimate purposes
  ➢ Adequate, relevant and limited
  ➢ Accurate (and rectified if inaccurate)
  ➢ Not kept for longer than necessary
  ➢ Processed securely – to preserve the confidentiality, integrity and availability of the personal data

• Data controller must be able to demonstrate compliance with principles
Rights

- Rights of:
  - Being informed about how personal data are used (usually via a detailed ‘privacy notice’ covering prescribed topics)
  - Access
  - Rectification of inaccurate personal data
  - Restriction pending verification or correction
  - Objection (including to profiling and direct marketing)
  - Erasure (‘the right to be forgotten’)
  - Portability

- All rights are qualified, and DPA 2018 adds numerous specific exemptions
Accountability

• Focus in GDPR on accountability measures
  - Data Protection Impact Assessments for ‘high risk’ processing
  - Prescribed contents of contracts with data processors, including transfers outside the EEA
  - Maintenance of a personal data register
  - Reporting certain personal data breaches to ICO within 72 hours
  - Newly prescribed role of independent Data Protection Officer
Relevant exemptions for academic research

• One set of exemptions for **research purposes** – but only if:
  ➢ Complying with standard provisions would seriously impair the research
  ➢ No damage or distress to data subjects
  ➢ No individual decision-making about data subjects
  ➢ Safeguards are in place e.g. pseudonymisation

• Another set of exemptions for **academic expression** – but only if:
  ➢ Complying with standard provisions would be incompatible with the academic purpose
  ➢ A publication is envisaged
  ➢ That publication will be in the public interest
Research purposes exemptions

- Will be applicable for most academic research involving human participants and secondary personal data use.
- Two principles disapplied: can use personal data collected for other purposes for research ones, and can keep personal data indefinitely.
- Rights largely disapplied.
- But:
  - Still need a legal basis (‘a task carried out in the public interest’).
  - Still need to supply participants with a privacy notice.
  - Still need data management plans (e.g. minimisation, security, access).
  - Still need to comply with University research ethics policies, including ethical review where required, as an accountability measure.
Academic expression exemptions

• Will be applicable for most academic research that is akin to journalistic writing – aim is to protect freedom of expression

• All principles disapplied

• All rights (including supply of a privacy notice) disapplied

• But:

  ➢ Still need to comply with University research ethics policies, including ethical review where required, as an accountability measure
Further information

• Websites
  
  https://www.information-compliance.admin.cam.ac.uk/data-protection
  
  https://www.research-integrity.admin.cam.ac.uk/academic-research-involving-personal-data
  
• Email
  
  data.protection@admin.cam.ac.uk