Ethical and legal context for managing and sharing data from human participants

Veerle Van den Eynden

UK Data Service

University of Essex

Managing and sharing research data: What is new with the GDPR?

4 May 2018

UK Data Service

Drivers for sharing data

- Drive for openness and sharing – value and transparency
- Technological advances - easier for digital data to be discoverable and accessible
- Sharing data - fundamental in collaborative and multi-stakeholder projects

Enable optimal data sharing through the research lifecycle

Open where possible, closed when necessary

Ethical research

.....

“do no harm”

Ethical arguments *for* sharing data

- Not burden over-researched, vulnerable groups
- Make best use of hard-to-obtain data, e.g. elites, socially excluded, over-researched
- Extend voices of participants
- Provide greater research transparency

In each, ethical duties to participants, peers and public may be present

Ethical obligations and data sharing

- Research with human participants usually requires ethical review (Research Ethics Committee)
- Avoid social and personal harm
- Uphold scientific standards
- Comply with relevant laws
- Data repositories such as UK Data Service facilitate ethical re-use of research data, protection of participants and safeguarding of personal data:
  - data anonymisation
  - regulate data access
  - data sharing is NOT violation of data privacy or research ethics

Legal compliance

Duty of confidentiality and data sharing

- Duty of confidentiality exists in UK common law and may apply to research data
- information given in circumstances where it is expected that a duty of confidence applies, cannot normally be disclosed without the information provider's consent
- Disclosure of confidential information is lawful when:
  - the individual to whom the information relates has consented – consent for data sharing
  - disclosure is necessary to safeguard the individual, or others, or is in the public interest
  - there is a legal duty to do so, for example a court order

General Data Protection Regulation (GDPR)

- 25 May 2018
- Applies to:
  - any EU researcher (data controlers / data processors) who collects personal data about a citizen of any country, anywhere in the world
  - A data controller or data processor based outside the EU but collecting personal data on EU citizens
- Applies only to 'personal data': any information relating to an identifiable (living) person who can be directly or indirectly identified in particular by reference to an identifier
- Anonymised or de-identified data is NOT personal data so GDPR does NOT apply

GDPR principles for processing personal data

1. Process lawfully, fair and transparent

   Inform participant of what will be done with the data, process accordingly

2. Keep to the original purpose

   Collect data for specified, explicit and legitimate purposes

   Do not process further in a manner incompatible with those purposes

3. Minimise data size

   Personal data collected should be adequate, relevant and limited to what is necessary

4. Uphold accuracy

   Personal data should be accurate and kept up to date

5. Remove data which aren't used

6. Ensure data integrity and confidentiality

   Protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using appropriate technical or organisational measures

GDPR data subject rights

- The right to be informed
- The right of access
- The right to rectification (correction)
- The right to erasure (right to be forgotten)
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated individual decision-making and profiling

Grounds for processing personal data

One of these must be present to process a data subject's personal data:

- Consent of the data subject
- Necessary for the performance of a contract
- Legal obligation placed upon controller
- Necessary to protect vital interests of the data subject
- Carried out in the public interest or is in the exercise of official authority
- Legitimate interest pursued by controller

GDPR research exemption

Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is not considered to be incompatible with the initial purposes

Appropriate safeguards, e.g.

- data minimisation
- pseudonymisation

Principles 2 and 5 less strict:

- Purpose: further processing of personal data allowed (2)
- Personal data may be stored for longer periods (5)

Best practice for legal compliance in research

- Investigate early which laws apply to your data
- Do not collect personal or sensitive data if not essential to your research
- Seek advice from you research office
- If you must collect / handle personal or sensitive data:
  - be transparent about processing personal data
  - minimise the collecting of personal data
- Remember: not all research data collected from participants are personal data !

Strategy for sharing research data obtained from people

1. Obtain informed consent, also for data sharing and preservation or curation
2. Protect identities e.g. anonymisation, not collecting personal data
3. Regulate access where needed (all or part of data) e.g. by group, use or time period
4. Securely store personal and sensitive data

What's new with GDPR

- Principles, rights of data subjects and processing grounds for processing personal data are largely the same as under DPA, but much more explicit
- Emphasis on transparency, clear information, clear documentation
- Extra rights of subjects: data portability
- Reuse for research allowed with safeguards

Transparency when collecting personal data

	Personal data obtained directly from participants	Personal data obtained indirectly
Name and contact details of data controller (entity that determines the reason for processing personal data) and data protection officer	✓	✓
Purposes of the processing and legal basis	✓	✓
Categories of personal data concerned		✓
Who will receive or have access to the personal data	✓	✓
How long the personal data will be stored	✓	✓
The data subject's rights (access, correction, removal,…)	✓	✓
The right to lodge a complaint with the ICO	✓	✓
Source from which the personal data originate, and if applicable, whether it came from publicly accessible sources		✓
Whether providing personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
Any automated decision-making, and, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject	✓	✓
Safeguards for transfers out of Europe	✓	✓