
Ethical and Legal Context for Managing and Sharing Data from Human Participants

Dr Scott Summers

UK Data Service

University of Essex

Managing and Sharing Research Data: Best
Practice for Data Protection – Lift, London

28th and 29th November 2018



What is the UK Data Service?

- Funded by the ESRC
- Single point of access to a wide range of secondary social science data
- We provide support and training for data creators with accessing, managing, sharing and using data
- Delivered by staff based at universities across the UK (Essex, Manchester, Leeds, Southampton, Edinburgh and UCL)
- UK Data Archive – manages the UK Data Service and curates the data

Some statistics about the UK Data Service

- **7,277** datasets in the collection
- **1034** qualitative and mixed methods collections
- **400** new datasets added each year
- **219** case studies of data reuse
- **25,000** registered users
- **60,000** downloads worldwide per year
- **4000+** user support queries per year

Why share data? (1)

- Increasing drive for openness, research transparency and sharing (linked to journal and funder requirements)
- Maximise return on investment and making optimal use of publicly funded research
- Avoid duplication of data collection
- Not burden over-researched, vulnerable groups and make best use of hard-to-obtain data, e.g. elites and socially excluded
- Extend voices of participants

Why share data? (2)

- Better science
- Technological advances – easier for digital data to be discoverable and accessible
- Visibility for researchers
- Societal benefits

Too difficult to share data widely?

Ethical, legal and research integrity challenges

- Personal, confidential or sensitive information
- Linkage of data in multi-disciplinary projects
 - Difficult to conceal identity of participants / fieldwork locations
- Lack of trust in others mis-using data
- Beaten to publication

Ethical research

.....

“do no harm”

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 need not be a 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
- Best practice is to avoid vague or general promises in consent forms

Data protection considerations – the GDPR (1)

- The General Data Protection Regulation (GDPR)
- New EU-wide data protection regulation
- Came into force 25 May 2018
- The GDPR gives data subjects **greater control** over their personal data, whilst **modernising** and **unifying** European data protection rules
- **Clarity, transparency** and **accountability**
- The Data Protection Act 2018

Data protection considerations – the GDPR (2)

- Personal data is defined as ‘any information relating to an identified or identifiable natural person’ (‘data subject’)
- Living persons
- Though there may still be ethical reasons for wanting to protect this information
- Anonymised data is **not** personal data so the GDPR does **not** apply
- Applies to:
 - any **EU researcher** (data controller) 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

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 are not used

6. Ensure **data integrity and confidentiality**

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

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

The GDPR research exemption

- Public interest
- Scientific
- Historical research
- Statistical purposes

Appropriate safeguards, e.g.

- Data minimisation
- Pseudonymisation
- Technical and organisational measures

Grounds for processing personal data

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

1. Consent
2. Contract
3. Legal obligation
4. Vital interests
5. Public interest
6. Legitimate interest

Copyright



- Copyright is internationally recognised form of intellectual property right, which arises automatically as a result of original work such as research
- Copyrighted output from research could include spreadsheets (and other forms of originally selected and organised data), publications, reports and computer programs
- Copyright will not cover the underlying facts, ideas or concepts, but only the particular way in which they have been expressed
- The right will lie with the author of the work, or with their relevant institution — different universities will have different policies on intellectual property
- A copyrighted work cannot usually be published, reproduced, adapted or translated without the owner's permission

Copyright – key considerations



- Questions to ask:
 - Who the copyright holder of the datasets is?
 - Are you allowed to use them and in what way?
 - Are you allowed to archive and publish them in a data repository?
- Key considerations
 - Joint ownership
 - Datasets created by multiple researchers
 - Derived datasets
 - Database rights
 - Provision in a contract
 - Repository copyright rules

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 your 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!

How to share data obtained from participants in a legal and ethical way

1. **Obtain informed consent**, for data sharing and long-term preservation/curation
2. **Protect identities** through anonymisation and not collecting personal data for admin
3. **Regulate access** where needed (all or part of data) e.g. by group, use or time period

- * Store personal or sensitive data **securely** and separately*
 - (Utilise encryption and consider the storage location)

Questions

Contact Details:

Scott Summers

UK Data Service

University of Essex

ukdataservice.ac.uk/help/get-in-touch

