THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Operational

Data Protection and research

This is a guidance note for researchers at the School working with personal data. The Data Protection Act (DPA) covers how personal data should be processed. Personal data is any information that identifies a living individual, including opinions about that individual and/or any intentions a data controller has towards that individual. Personal data collected and used for research is covered by the DPA. However, the School's Research Ethics policy also applies, and covers personal data relating to the deceased.

The important sections of Data Protection Legislation for research are:

- six data protection principles that govern how personal data should be processed
- the lawful bases under which research data can be processed
- Rights relating to making requests
    - for information held
    - to have information corrected
    - to have information deleted

Researchers have to consider how they manage personal data from the point they start collecting it, through storage to disposal. What you tell research subjects about your project when it starts could determine how and where you could deposit the data at the end of it.

JISCLegal is also producing guidance, which will be linked to when it is available.

The Data Protection principles and research

1 processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
Personal data must be collected and used in accordance with Data Protection legislation. This principle means that individuals should know who is collecting the research, where it will be kept and what will be done with it. If you are collecting the data, you should have a privacy notice on the form or associated with the collection so that people are aware of what you will be doing with their data. The School's Informed Consent guidance is here: https://info.lse.ac.uk/staff/Services/Policies-and-Procedures/Assets/Documents/infCon.pdf.

Part of lawfulness is identifying a lawful basis for processing the data. It is most likely that for research these will be:

- Consent, which must be unambiguous and can be withdrawn at any time.
- Public interest, which would cover research conducted in the public interest. You would need to record what this public interest is.
- Legitimate interests, which can be used for research not covered by the two lawful bases above.
- Contract, which may apply if you are doing consultancy work in an organisation. You are likely to need consent if your research involves people outside that organisation for your consultancy work.

There may be some research projects where gaining informed consent is not possible or very difficult e.g. anthropological research where observation is the mode of research and gaining consent would interfere with the observation. Legitimate interests is likely to apply as long as the research subjects' data is anonymised and will cause them no harm to process. The Association of Social Anthropologists ethical guidelines contain a useful list of issues to consider when negotiating consent for research as well as what to avoid in Section 1 (4) and (5). The British Sociological Association's statement of ethical practice also offers guidance in this area.

Care needs to be taken to ensure that consent is meaningful and freely given. Employees who have been told to participate in research by their organisation cannot be said to have freely consented to participating in research. Some children and vulnerable adults may be able to consent, but parents and guardians may need to give consent on their behalf.

Special categories data have their own lawful bases and are covered below.

2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');.

If you are reusing a research data set someone else has collected for further research, the exemption under Article 5(1)(b) shown above applies. This section allows for any personal data to be reused in research providing that it is not incompatible with the previous purpose. We have no case law or guidance regarding what would be incompatible in this area yet.

If you are being required by a research funder or intend to deposit the data in an open repository in anonymised or any other form so it can be used by other researchers, tell research subjects you are doing so when collecting the data.

3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

Only collect the personal data you really need for your project. Consider what is really necessary for your project before you start as to get informed consent (see above) you will need to explain to research subjects why you need their personal data.

4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

Personal data collected for research is likely to be a snapshot of a moment in time. As such, it is unlikely to need updating. Long term collections will be keeping to this principle anyway for the purposes of future research.

5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')

So research data is exempt from principle 5 as long as data subject rights and freedoms are safeguarded. This doesn't mean that you shouldn't consider how long to keep data. You should consider destruction of the original dataset once an anonymised or other form is in an open digital repository, for instance.

6 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

Personal data should be kept securely so that no unauthorised access can occur.

Paper/hard media should be:

- kept in lockable cabinets/cupboards when not in use
- kept in lockable offices if possible
- not left lying on desks if you will be away from your desk for a considerable period of time

Electronic data should:

- Not be displayed where third parties can inadvertently see it
- Not be forwarded to third parties accidently – always check email addresses
- Be encrypted or password protected in transit
- Be kept on secure network drives or password protected/encrypted removable media.
- Once the School provides an extra secured area on the network, research data that has either of the following characteristics should be stored in the extra secured area:
    - been specifically required by a research funder to have extra security OR
    - contains sensitive personal data
    - needs the extra security in the opinion of the Information Security Manager and/or Information Rights team

Processing special categories personal data

The GDPR defines certain data as being sensitive personal data, requiring more stringent processing. The sensitive personal data are:

- Race or ethnic origin

- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Biometric and genetic information
- Criminal or alleged criminal offences
- Participation or alleged participation in court proceedings

Article 9 of the GDPR has its own lawful bases for processing this data. One of these is explicit consent, but the other that can be used by researchers is 'j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.' So if using the data is proportionate for the research and the fundamental rights and interests of the data subject are safeguarded, Article 9(2)(j) allows for processing of this data for research.

Explicit consent means you must be able to prove that the research subject knew what was being collected, how it would be used and how the data would be disposed of at the time it was collected. This means you will need a signature or mark on a form or bottom of a letter explaining the research or a tick box on an electronic form will need to be ticked.

Requests for information – Subject Access requests, corrections and erasures

Research subjects have two major rights under the DPA. The first is to request any information held on them and the second is to have erroneous information corrected or deleted. The School has never received either type of request from a research subject, but both remain a possibility.

Subject access requests are handled by the Information Rights team. A research subject that indicates to you that they want a copy of the data held on them should be directed to the email address glpd.info.rights@lse.ac.uk. We will process the request, which will involve filling out a form and providing the £10 fee and proof of ID. We have 40 days from receipt of the fee to provide any information held. Researchers will need to send the Information Rights team a copy of any information held as soon as possible, but no later than 39 days after the fee is received.

Requests for corrections and deletions have to be dealt with within 21 days. However, this means we must respond within 21 days. If a researcher has evidence that the information they hold is correct, the research data does not necessarily need to change. However, a note should be added to the effect that the research subject has challenged the accuracy of the data. While a research subject can ask for their data to be removed from a dataset, it will be very difficult to do so once the research has been published. There are no test cases in law for this situation. It could be a case of noting in any further research products that the dataset is slightly different if the data does need to be removed.

Anonymisation and Pseudonymisation of research data

Anonymisation should mean that a dataset has been cleared of any potentially identifying data before being published and/or released to third parties. However, true anonymisation is difficult to

achieve if a dataset is to be useful for reuse. An ability to remove identifying data satisfactorily can lead to a pseudonymised data set, which has the obvious identifying data removed but leaves enough for a third party to identify the individual research subjects. As such, it is worth letting research subjects know if their data will be included in a published dataset and what you plan on including so as to minimise their identification.

The Information Commissioner's Office produced a code of practice for Anonymisation, which also includes methods for anonymising data.

Transfer outside the EU and working with collaborators

The GDPR does not allow transfer of personal data outside the EU or a country with adequate protection without meeting a condition like explicit consent or binding contract.

So, get explicit consent for sending data outside the European Economic Area (the EU plus Norway, Iceland and Liechtenstein) if you are at all likely to be processing it outside those countries. You should be fairly safe in countries like Canada, Switzerland, US organisations covered by the EU/US Privacy Shield and some other countries listed by the EU, which have received adequacy decisions. Use password protection or encryption where possible in transit, but bear in mind that some countries will require you to provide the encryption keys if you take personal data into them.

An alternative to transmitting data is to use SharePoint or OneDrive as this keeps the data within the EU. You can organise external collaborator accounts for external researchers. This is particularly recommended for countries without adequate protection. Collaborators in EU countries will already be subject to GDPR.

Summary of Data Protection issues for research

You need to provide research subjects the following:

- The name of the project, its purpose and objectives.
- The identities of the organisations or individuals who have funded the research, and any interests they may have in the research.
- Why the information is being collected, and why it is necessary for the project.
- The name and contact details of the person who will be responsible for the data gathered in the project (usually, the researcher).
- Who will have access to the data, including any organisations or individuals outside the School who may be given access.
- Any special security measures which will be taken to protect the data.
- The countries to which the data may be transferred, including the fact that the data will be transferred to the UK (if the data is gathered outside the UK), and whether the data may be transferred outside the EEA.
- How the data will be published or made available, including whether research subjects will be identifiable in the published data, or whether the data will be published in anonymised form.
- Steps which will be taken to archive the data, e.g. by depositing a dataset in a data archive (e.g. one specified by the research funder or with the School), and whether the archived data will be anonymised or non-anonymised.
- How the data may be used in future research projects.
- How the research subject can withdraw their consent to participate in the project if they subsequently decide to do so.

Contacts

Rachael Maguire; email r.e.maguire@lse.ac.uk
OR glpd.info.rights@lse.ac.uk

Review schedule

Review interval	Next review due by	Next review start
3 years	30/09/21	01/09/21

Version history

Version	Date	Approved by	Notes
2	24/09/18	Data Protection Officer	Update for GDPR

Links

Reference	Link
N/A	N/A

Contacts

Position	Name	Email	Notes
Rachael Maguire	Data Protection Officer	glpd.info.rights@lse.ac.uk	

Communications and Training

Will this document be publicised through Internal Communications?	~~**Yes**~~**/ No**
Will training needs arise from this policy	**Yes/ ~~No~~**
If Yes, please give details Data Protection and Research, through the Library.	