

University of London

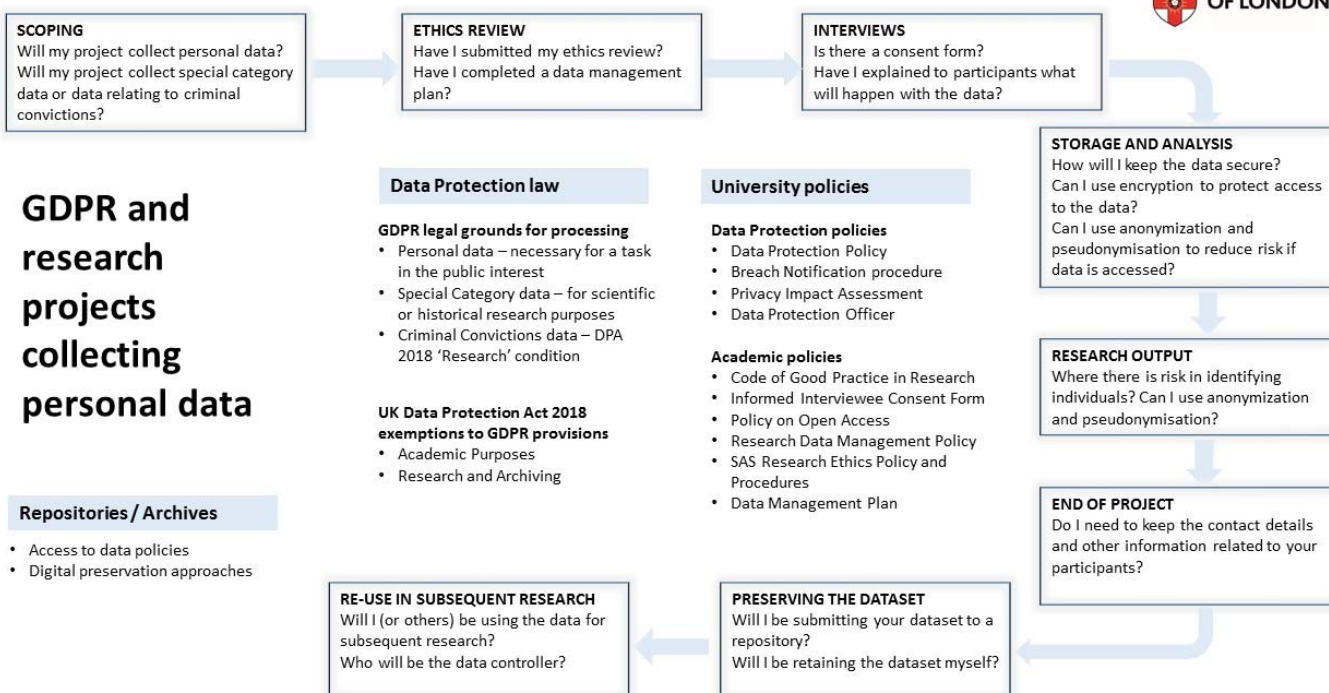
Guidance on data protection and research

Contents

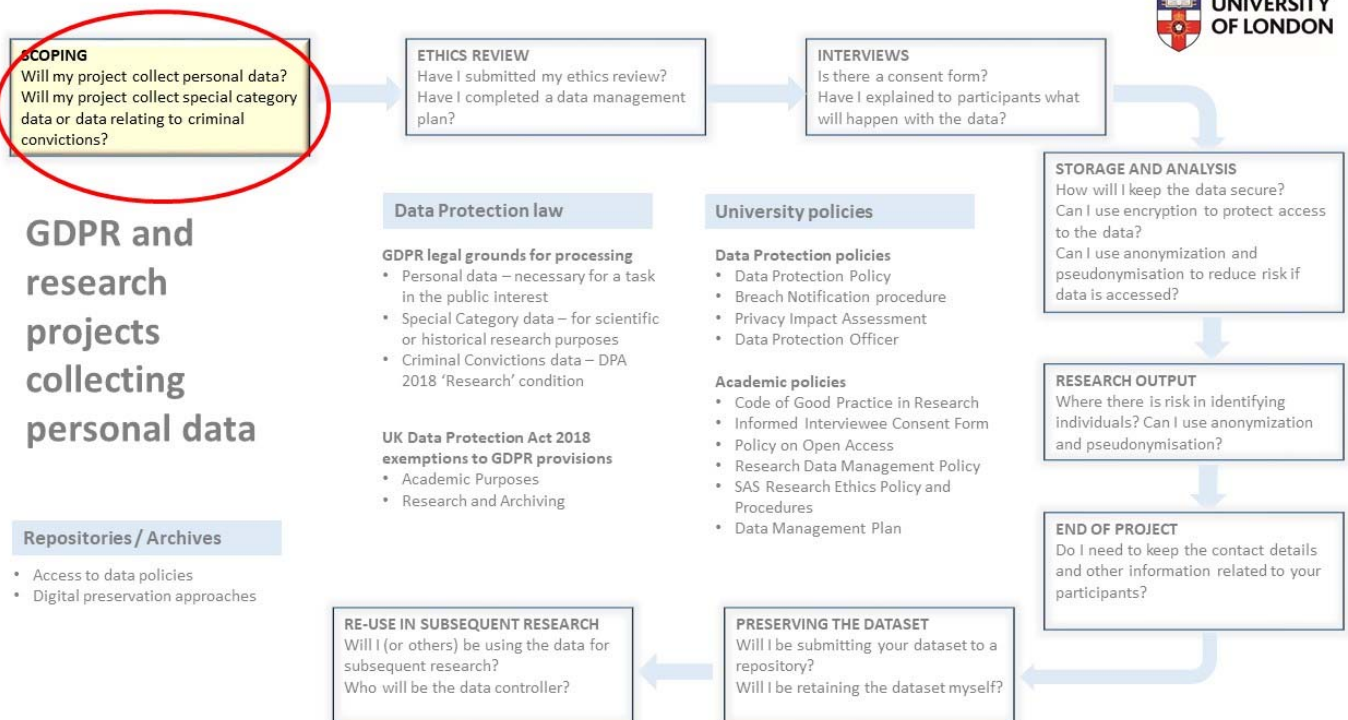
1. Purpose of this document.....	3
2. Scoping a research project.....	4
3. Ethics Review	7
4. Interviews.....	8
5. Storage, analysis and output	10
6. The End of the project	12
7. Preserving the dataset	13
8. Transferring to a repository	14
9. Associated policies and guidance and forms.....	15
10. Further Information	15
11. Version control.....	15
12. APPENDIX A – Definitions.....	16
13. APPENDIX B – Legal grounds for processing	17

1. Purpose of this document

This document provides guidance on managing personal data in academic research. It provides a commentary on the various stages of a research project, as set out in the diagram below. Each section will look at a different stage. Please read in conjunction with the University's research policies and research ethics approach.



2. Scoping a research project



There are two key pieces of legislation to consider:

- The General Data Protection Regulation became live in May 25 2018
- UK Data Protection Act 2018 – implements the GDPR and adds UK definitions on areas specified by GDPR



There a number of definitions in the law provided in Appendix A at the end of this document.

The Data Protection Principles

The University is required to process personal data according to the following six principles:

Data Protection Principles	The context for research at the University
<i>Lawfulness, fairness and transparency</i>	The researcher explains to their interviewees how they processes personal data at the point of collection, what the legal basis is for processing and for what purposes the data will be used. In circumstances where the data is not sourced from the individual, information is made available which explains how the data is used.
<i>Purpose limitation</i>	The researcher only uses the personal data it has for the purposes it was collected for, unless certain safeguards around re-use apply.
<i>Data Minimisation</i>	The researcher only collects personal data which is relevant to the purposes it is required for, unless certain safeguards around re-use apply.
<i>Accuracy</i>	The researcher ensures that the data is correct, up to date and able to be rectify any mistakes quickly
<i>Storage Limitation</i>	The researcher does not retain personal data for longer than it is needed, unless certain safeguards around long term or permanent storage apply.
<i>Integrity and Confidentiality</i>	The researcher protects their personal data against unauthorised access, loss or destruction by a range of security measures.

Types of data subjects in research

The data subjects in research will likely fall into two categories:

- Individuals who provide a unique set of data directly (or via a mediator) to the researcher as part of a project, such as an audio interview, a questionnaire or a series of actions that give results (e.g. results from a physical or mental test)
- Individuals whose data is obtained by a researcher from primary source material or secondary literature (e.g. researching a living political figure from contemporary media or biographies, collating public social media handles and statements)

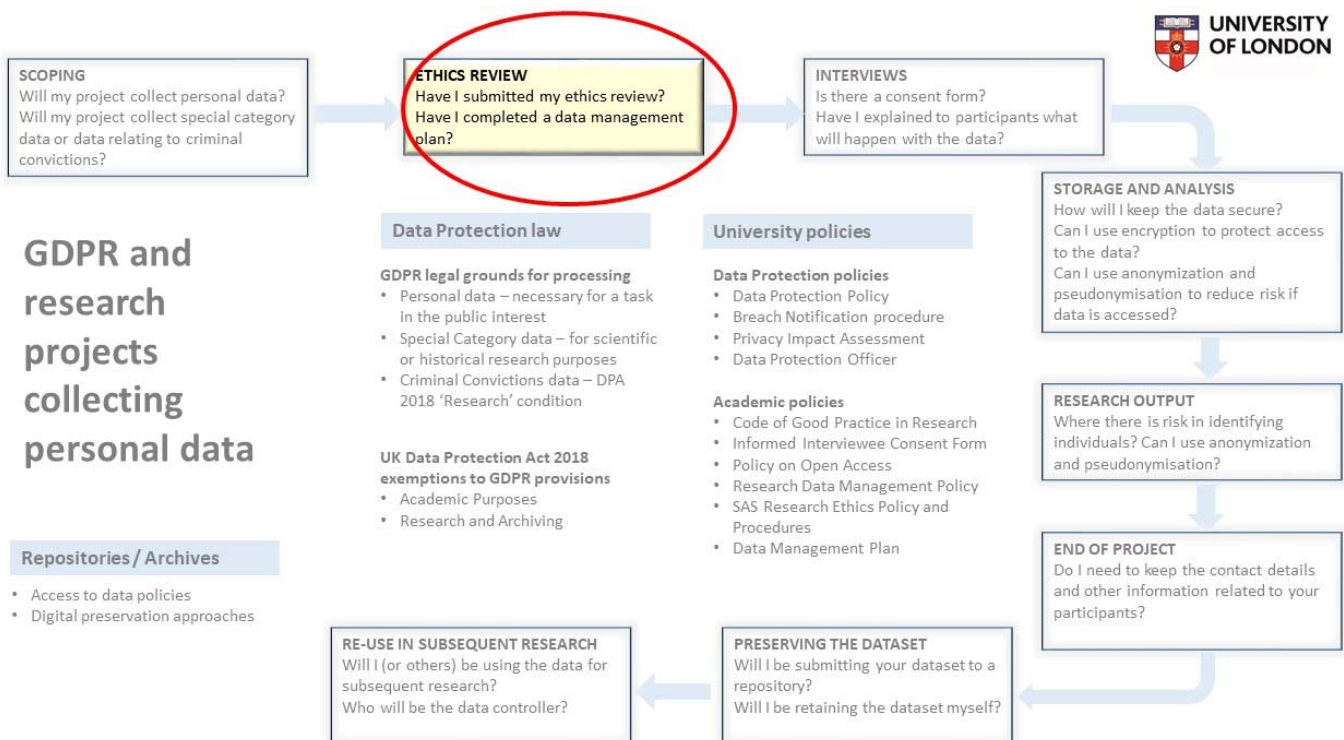
As might be expected, the research participant requires more consideration in regards to managing personal data in the context of GDPR.

Data protection law recognises the need to balance these rights with the requirements of pursuing academic research and there are a range of exemptions that a researcher can apply.

The Rights of individuals

Data subjects – in the research contexts participants and other living individuals referred to in research – have a number of rights under the GDPR but these are substantially qualified by exemptions in the Regulation and the UK Data Protection Act 2018. These can be found in the Appendices. The key message for researchers is to keep participants fully informed about what is being done with their data, be responsive to concerns and, where possible in the context of the research, be prepared to withdraw or remove their data from the project.

3. Ethics Review



Are there ethical questions to consider around the data I'm collecting? Have I checked this with my supervisor or the relevant University board?

Please note that it is part of the University's policy that all academic researchers must submit seek ethical approval before undertaking their research. For more information:

<https://www.sas.ac.uk/research/research-office/research-ethics>

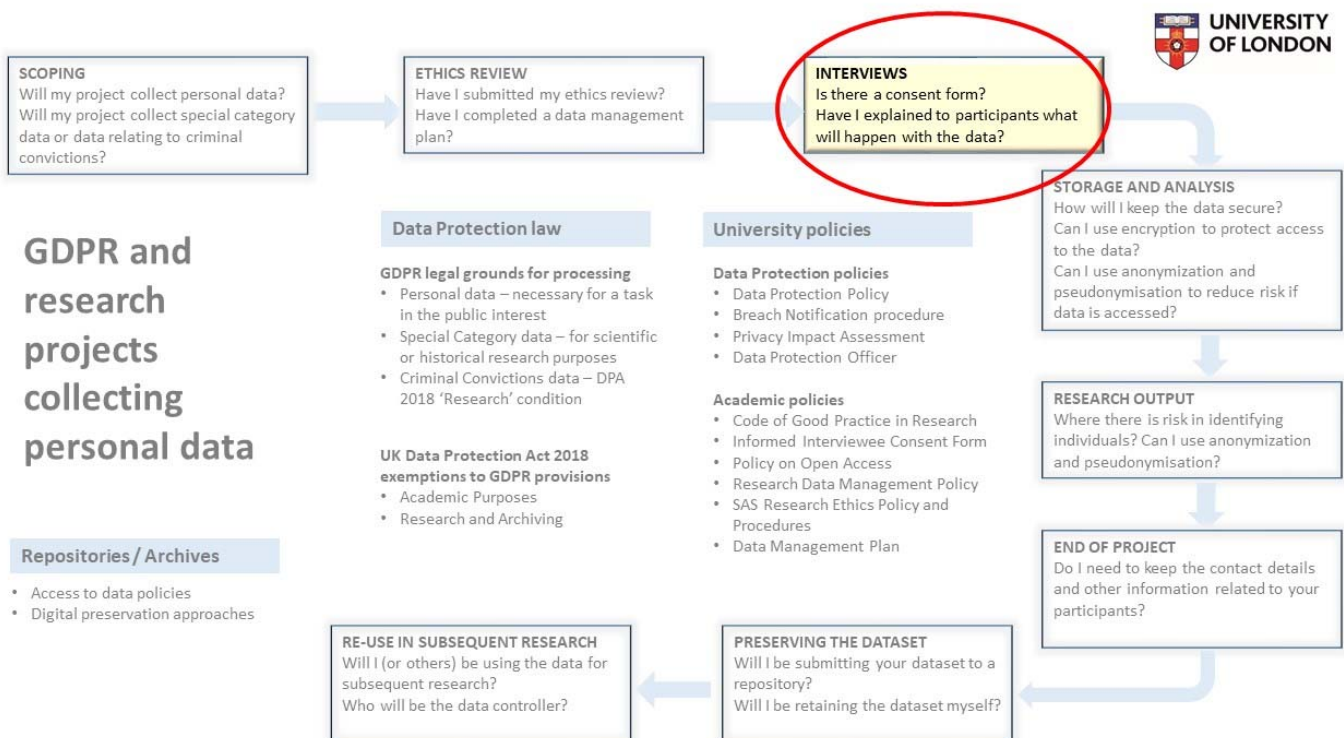
It is a good idea to complete a Data Management Plan:

- ensures that the data created in the research project is managed effectively
- defines what data is being created
- who is responsible for it
- how it is going to be stored and made accessible

The University's data management plan template can be found at:

<https://www.sas.ac.uk/research/research-office/research-ethics>

4. Interviews



Research ethics ‘consent’

The ‘consent form’ is a long established resource for academic researchers in working with participants and remains a vital part of the University’s procedures for research projects.

We need to ensure we provide as much information as we can to our participants. If we are to re-use data, they should understand who is collecting the data and the purposes it is being collected for. They should also be informed that research data:

- will be retained
- re-used by the researcher
- Re-used in other contexts (a repository, another researcher) whilst also explaining the safeguards that will be put in place to protect their rights and freedoms.

GDPR and the legal basis for processing

“Where the data subject has given consent” is one of the six legal bases available to process personal data in the General Data Protection Regulation (see appendix below for further information).

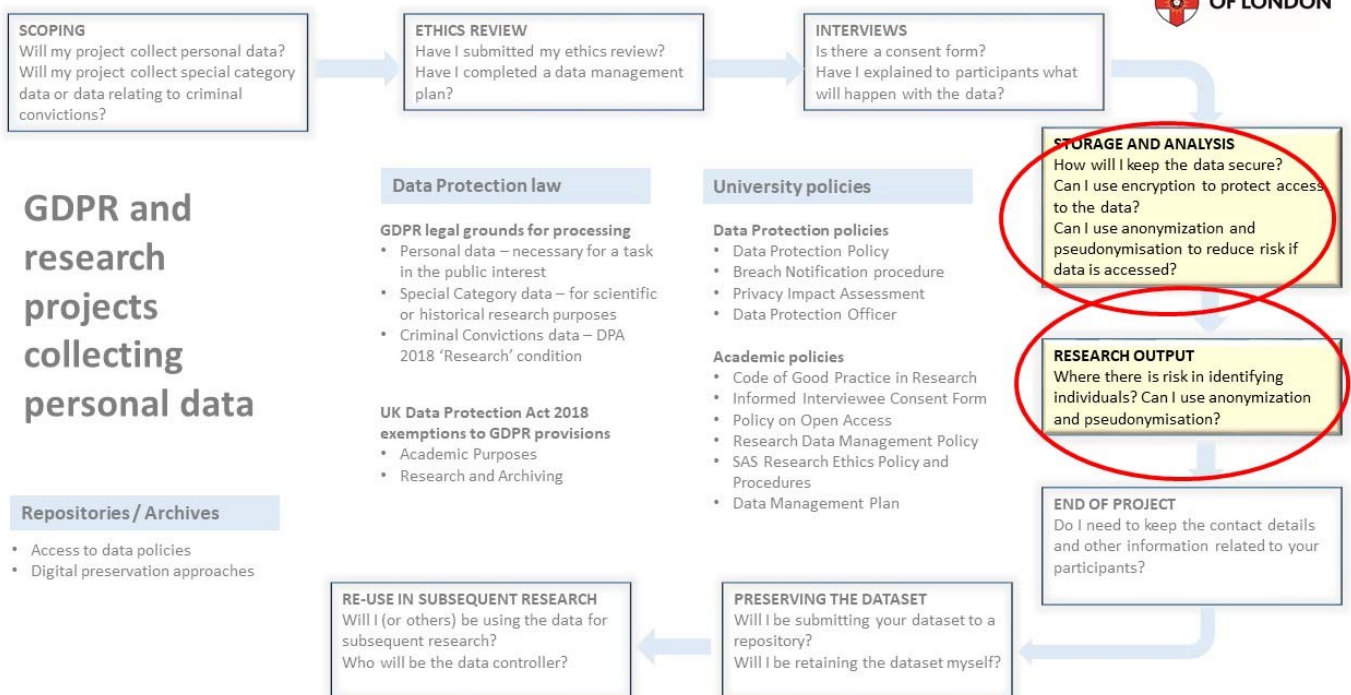
With research data GDPR consent becomes problematic where the individual wishes to retract the information, where the research participant might not be able to give fully informed consent or where there might be a power imbalance between the researcher and participant.

As stated in the University's 'Academic research and data protection policy', the University will rely on the following legal basis for processing personal data in research:

Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

The additional legal grounds to cover 'special category' or 'criminal convictions' data is defined in the University's policy/

5. Storage, analysis and output



The value of research data is recognised in the GDPR and privileged with a number of exemptions not afforded other types of personal data. Data controllers are, however, required to balance the use of personal data with a number of safeguards to protect the rights of data subjects.

"Necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes..."

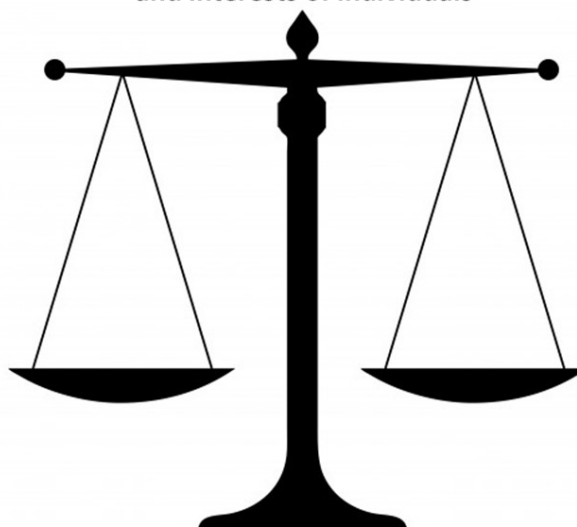
GDPR legal grounds for processing

- "Task in the public interest"
- "necessary for scientific or historical research purposes"

UK DPA 2018 Exemptions:

- Journalistic, academic, artistic and literary purposes
- Research and statistics
- Archiving in the public interest

GDPR: Balancing research with the rights and interests of individuals



...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"

Collection and analysis

- "Data minimisation" principle
- Transparency
- Pseudonymisation
- Anonymisation

Storage

- Controlled access
- Secure storage
- Encryption

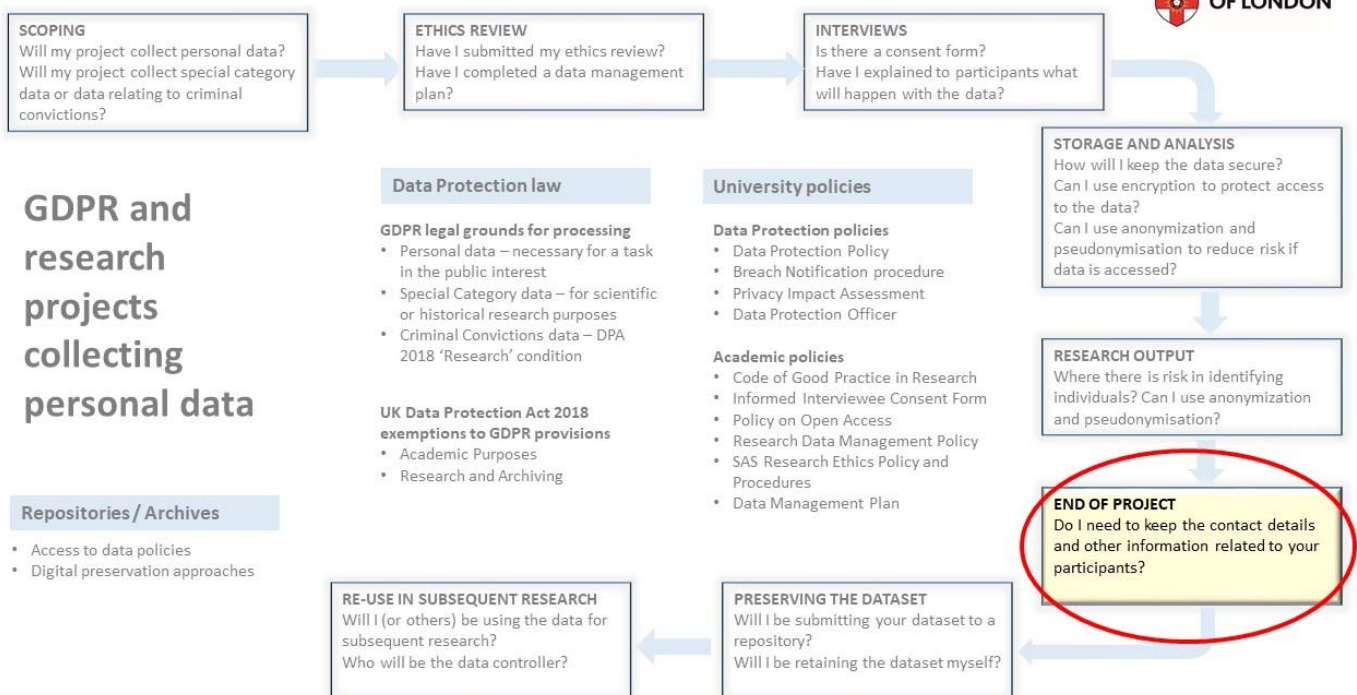
Analysis / Presentation

- Research does not
- identify individuals, where this does not affect the purposes of the research
 - lead to a decision being made that affects that individual

Whilst there is no single way to do this defined in the law, the general expectations would be as follows

How the data is analysed and presented	<ul style="list-style-type: none">• Research does not identify individuals, where this does not affect the purposes of the research• Research does not lead to a decision being made that affects that individual
How the data is stored	<ul style="list-style-type: none">• Data is, where possible, anonymised or pseudonymised (please see 'Appendix A' for further information).• Data is kept securely to guard against unauthorised access, loss or misuse• The principle of 'data minimisation' is observed• A plan to effectively preserve the data so it does not become obsolete

6. The End of the project



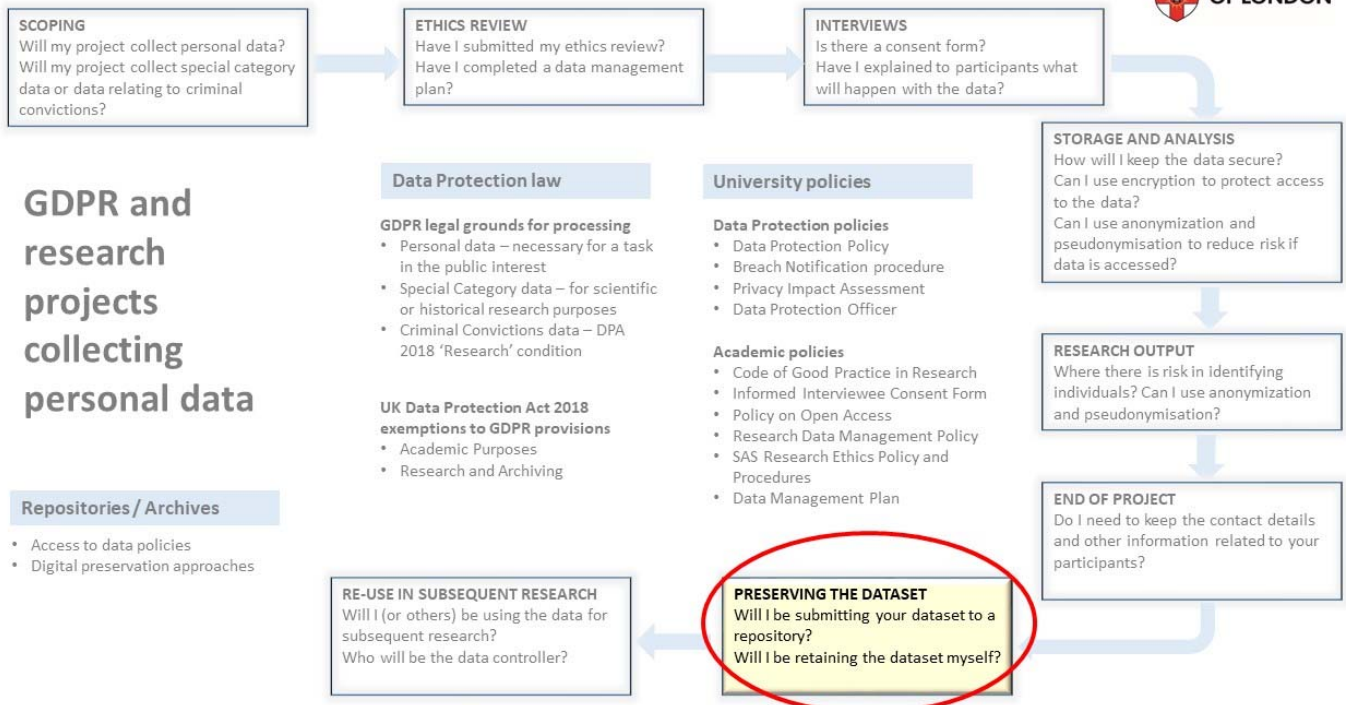
The end of a research project is just one more step in the lifecycle of your dataset.

There will be a number of records arising from your research project, typically fall into the following categories:

- Records documenting the management of the research project, such as applications for funding, invoices, staff records, correspondence
- Records documenting research outcomes or products, such as reports or monographs
- Research data in 'raw' and 'analysed' forms.

Whilst we are naturally concerned in this document with the data protection perspectives in regards to research data in 'raw' and 'analysed' forms, data protection law will also apply to the records developed in the management of the research project. This may include details and correspondence with participants that will be unrelated to the research data. You should review all these records to check how long you'll need to keep them. Holding onto records indefinitely can often result in unnecessary risk.

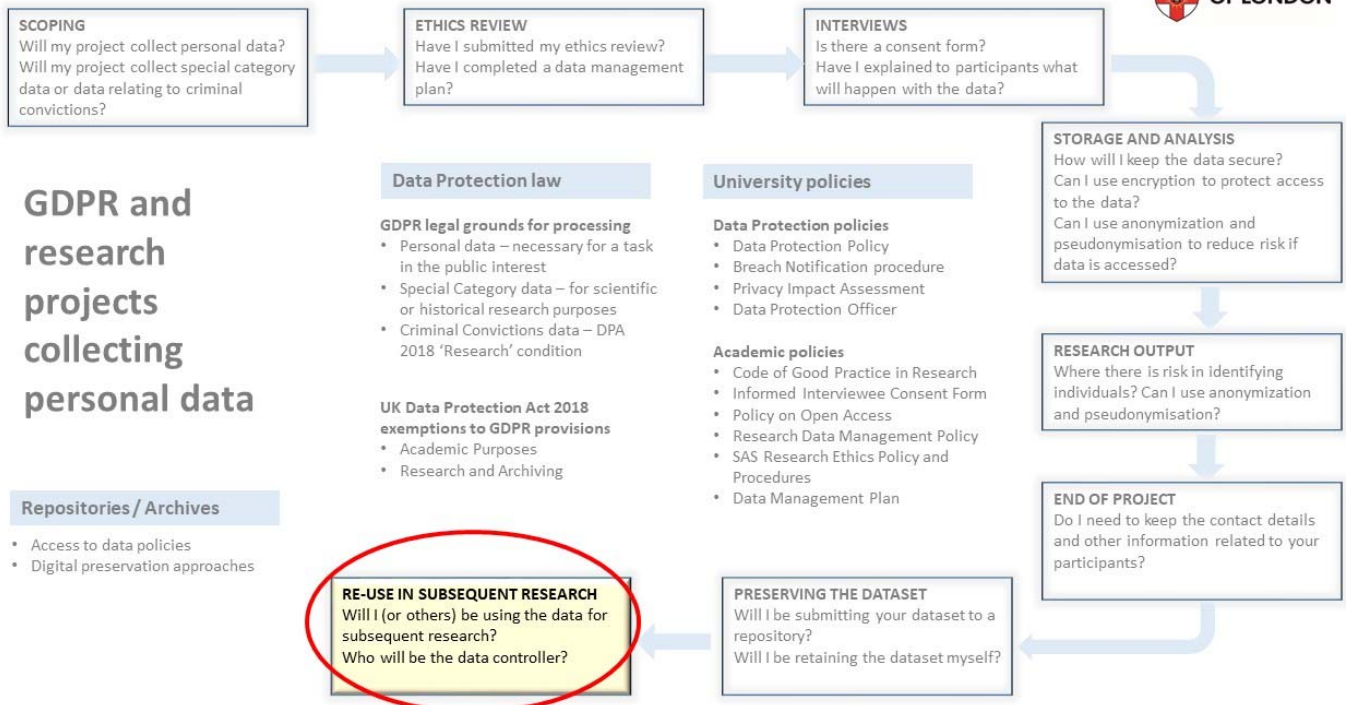
7. Preserving the dataset



There are a number of questions that need to be determined at this point:

- Is there a plan to effectively preserve the data so it does not become obsolete?
- Preservation is different from storage. An approach to the preservation of the data includes the following factors
- What format is the data in?
- What application / platform allows you to access this data?
- Will you still be able to run / access / open / analyse this data in 10 / 20 years' time (or longer)?
- Where will the data be kept?
- Are the research participants aware what will happen to their data when the research project ends?

8. Transferring to a repository



Many research grants require the dataset from the research to be submitted to a repository for storage and future use.

In these situations the repository becomes the data controller and the data is likely to be held according to new terms and conditions. The same requirements of legislation and safeguarding data will apply.

We should at the start of our project make sure that research data which relates to them:

- will be retained
- re-used by the researcher
- Re-used in other contexts (a repository, another researcher) whilst also explaining the safeguards that will be put in place to protect their rights and freedom

9. Associated policies and guidance and forms

University of London Data Protection Policy

University of London Information Security & Acceptable Use Policy

Academic Research and Data Protection Policy

Informed Interviewee Consent Form & Participation Information Sheet

Open Access Policy Research Data Management Policy

Data Management Template

Research Ethics Policy and Procedures

10. Further Information

Any questions relating to this policy should be directed to the Data Protection & Information Compliance Manager at: data.protection@london.ac.uk or the Head of Management Information and Research Services at: research@sas.ac.uk

11. Version control

Date	Version	Reason for change	Author
July 2018	0.1	Initial draft updated to comply with General Data Protection Regulation	Data Protection & Information Compliance Manager
February 2019	0.2	Based on feedback from Head of Research Services and Chair of Research Ethics Committee with Initial draft divided into shorter policy and separate guidance document for researchers	Data Protection & Information Compliance Manager
April 2019	0.3	Further discussion and feedback from Head of Research Services and Chair of Research Ethics Committee, changes including appendices	Data Protection & Information Compliance Manager

12. APPENDIX A – Definitions

The General Data Protection Regulation governs the processing of personal data. The following definitions are used in the Regulation and related legislation:

Personal data

- information relating to an identified or identifiable natural person ('data subject');
- can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- "this Regulation should not apply to deceased persons"

Special Category data

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

Criminal Convictions data

- personal data relating to criminal convictions and offences or related security measures

Processing

- 'processing' means any action that is performed on personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Data Subject

- the individual who is the subject of personal data – this would apply to interviewees in a research project or a living individual described or referred to in primary sources or secondary literature

Data Controller

- A Data Controller determines the purposes for which personal data are processed. The University is the Data Controller for research data at the University, though other organisations may act as controllers of research data at various times (please see below)

Data Processor

- A Data Processor is any individual or organisation who processes personal data on behalf of – and according to the purposes defined by – the data controller

Pseudonymisation

- 'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information,

provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the person is not identified

Anonymisation

- Means the processing of personal data in such a manner that it no longer becomes possible to link the data back to the individual and therefore ceases to be personal data and in the scope of GDPR.

Encryption

- Encryption re-codes data in such a way that it is only accessible to those who are given the key to open the files. A common approach would be to use password protected files for storage and transfer or encrypted removable media such as a portable hard drive or USB stick. Encryption is increasingly seen as a minimum standard for safeguarding data.

13. APPENDIX B - Legal grounds for processing

The six lawful grounds for processing personal data under GDPR are as follows:

Legal Grounds / Lawful Basis for processing data	Context for research
Where the data subject has given their consent	GDPR consent is different from 'consent' as established in research ethics and is therefore unsuitable as a legal basis for academic research
Where it is necessary for the performance of a contract	Typically the basis of the University processing the employment data of its staff or registry data of its students and therefore unsuitable as a legal basis for academic research, unless individual is being paid to participate
To protect an individual's vital interests	Usually reserved for medical emergencies or serious welfare or safeguarding issues and not suitable for academic research
For the performance of a legal obligation	Not suitable for academic research
For the performance of a task in the public interest or in the exercise of official authority vested in the controller	This is defined in the University's policy as the legal grounds it relies on for the processing of personal data in academic research
For the 'legitimate interests' of the data controller or another third party, balanced against the rights and freedoms of the individual.	The University can only rely on this grounds for processing where it is not acting wholly as a 'public authority' (e.g. non-academic research, commercial activities)

14. APPENDIX C – Research exemptions around the rights of individuals

GDPR Right	The potential context for research	Exemption in the case of academic research
<i>Transparency</i>	The University is required to “take appropriate measures to provide” a privacy notice relating to the processing to the data subject “in a concise, transparent, intelligible and easily accessible form, using clear and plain language”. This is straightforward in terms of a research participant signing a consent form but is more difficult in regards to the personal data of living individuals generated by a researcher from primary source material or secondary literature.	Article 14 (5) (b) GDPR No requirement to provide privacy notice where “the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes” where providing this information “is likely to render impossible or seriously impair the achievement of the objectives” of the research.
<i>Right of access</i>	A research participant has the right to find out about what we are doing with their data, check we’re holding it correctly and to obtain a copy of what we hold.	<i>Research and Statistics DPA</i> Sched 2 (6) (27) (2) <i>Academic purposes DPA</i> Sched 2 (6) (27) (9) (b)
<i>Right to rectification</i>	If a research participant thinks something we hold about them is wrong, they can ask for this to be corrected. The researcher will assess the request and correct any inaccuracy.	<i>Research and Statistics DPA</i> Sched 2 (6) (27) (2) 15 <i>Academic purposes DPA</i> Sched 2 (6) (27) (9) (b)
<i>Right to erasure / right to be forgotten</i>	Research participants have the right to ask us to remove or delete data we hold on them. The University will assess the request against the criteria in Article 17 and respond accordingly.	Article 17 (3) (b) <i>Academic purposes DPA</i> Sched 2 (6) (27) (9) (b)
<i>Right to restriction of processing</i>	Research participants may, in the course of a dispute with the University about the use of their data, ask the University to stop using their data if certain criteria applies.	<i>Research and Statistics DPA</i> Sched 2 (6) (27) (2) <i>Academic purposes DPA</i> Sched 2 (6) (27) (9) (b)
<i>Right to data portability</i>	Research participants have the right to ask the University to provide them with a	Article 20 (3) - where the research processing is necessary

	re-usable electronic copy of their data to allow them to transfer it to another provider.	for the performance of a task in the public interest, then a request under this right can't be made. <i>Academic purposes</i> DPA Sched 2 (6) (27) (9) (b)
<i>Right to object</i>	Research participants have the right to object to processing based on legitimate interests, legal obligation or for the purposes of direct marketing or, in certain circumstances, "scientific or historical research purposes or statistical purposes". The University will assess the request and respond accordingly.	Article 21 (6) – where the research processing is necessary for the performance of a task in the public interest, then a request under this right can't be made. <i>Research and Statistics - DPA</i> Sched 2 (6) (27) (2) <i>Academic purposes</i> DPA Sched 2 (6) (27) (9) (b)
<i>Automated decision making, including profiling</i>	If the University is making decisions about data subjects through purely automated means, such as a computer algorithm, data subjects can appeal against this decision. The University will ensure that subjects can express their point of view and have member of staff provide a review and explanation of the decision.	<i>Academic purposes</i> DPA Sched 2 (6) (27) (9) (b)