DATA PROTECTION FOR RESEARCHERS

This document sets out the requirements for the collection, handling, storage and destruction of personal data used in research activities.

What is the General Data Protection Regulation? (GDPR)

The GDPR is Europe's new framework for data protection laws and will apply to the UK on 25 May 2018. Although it will replace the Data Protection Act 1998, much of the GDPR's concepts and principles are in line with the current data protection law. The GDPR gives new rights for people in relation to the information organisations hold about them, obligations for data management, and a new regime of fines if the GDPR is breached. Organisations outside the EU are subject to the GDPR when the data collected concerns EU citizens.

This guidance relates to all personal data held by the University of Reading (including the Henley Business School, subsidiaries and undertakings) and being handled by those working for or under the instruction of the University, including PGR students.

The University must ensure that handling of personal data used for research activities is done in accordance with our legal obligations including those set out in the General Data Protection Regulation, the Data Protection Bill (Act likely to be passed in 2018), the Privacy of Electronic Communications Regulations 2003 and Article 8 of the Human Rights Act. The requirements in this document set out the actions needed to ensure we can meet these obligations and offer guidance and advice on data protection compliance for researchers.

This document should be read in conjunction with guidance and advice on Research Ethics and is supplementary to any advice or requirements of the University Research Ethics Committee (UREC) and national Research Ethics Committees (RECs)

Executive Summary

This document sets out the legal basis for handling research data under the GDPR and data protection laws. It explains what participants need to be informed of when taking part in research studies, what areas of data use need consent, what safeguarding measures to protect data should be used, information on retention, deletion and anonymisation and where to go for advice. It also includes template consent and information sheets that can be used to guide researchers as to what must be covered to meet our obligations.

A checklist for researchers is contained within Appendix A

WHAT IS PERSONAL DATA

Data protection law defines personal data as being:

"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who 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."[1]

Data protection law defines special category (sensitive) personal data as being:

"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."[2]

The Data Protection Principles

If you are collecting personal data or personal sensitive data, its use will be subject to the following requirements.

Under data protection law we are required to ensure and demonstrate that personal data is:

1. used fairly, lawfully and transparently;

2. collected for specified, explicit and legitimate purposes;

3. adequate, relevant and limited to what is necessary for the purposes;

4. accurate and, where necessary, kept up to date;

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes;

6. kept secure with appropriate technical and organisational measures

This document explains these requirements and provides instructions on how to address them in research activities involving the use of personal data.

FAIRNESS, TRANSPARENCY, LIMITED AND SPECIFIC PURPOSES (PRINCIPLES 1 AND 2)

We are required by law to provide research participants with the following:

- The name and contact details of our organisation.
- The contact details of our Data Protection Officer.
- The purposes of the use of personal data.
- The lawful basis for the use of personal data.
- The categories of personal data obtained.
- The recipients or categories of recipients of the personal data (to include third parties the data may be shared with).
- The details of transfers of the personal data to any third countries or international organisations (if applicable).
- The retention periods for the personal data.
- The rights available to individuals in respect of their personal data.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority (for example the Information Commissioners Office).
- The source of the personal data (if the personal data is not obtained from the individual it relates to – exemptions from this requirement may apply to data passed to us by another for research purposes, seek advice from your Data Protection Officer if in doubt).

[1] General Data Protection Regulation (EU) 2016/679 Art 4 (1)
[2] General Data Protection Regulation (EU) 2016/679 Art 9 (1)

- The details of the existence of automated decision-making, including profiling (if applicable). More information on automated decision making can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

Transparency exceptions for personal data used for research purposes

"It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research."[3]

This means that where being explicit about the differing purposes of a study would be *prejudicial to the research* objectives or outcomes, you can be less specific. This only applies where the prejudice can be clearly evidenced and where this is the case, it should be explained in any research ethics or project documentation.

'Opt-out' approaches and transparency requirements

Transparency obligations should be considered for studies that involve informing participants of a research study to be undertaken and assuming they (or their children) are happy to take part if they do not object *(or opt-out)*.

We must be able to evidence that research participants were made aware of how their data would be used at the point is collected for research purposes. If you are embarking on a research project that uses an 'opt-out' approach to research *participation*, you must be confident that participants have read and understood this information and be able to *demonstrate* that this information was provided to the participants.

LAWFUL BASIS (PRINCIPLE 1)

Data protection law requires us to state our lawful basis for using personal data and communicate this to research participants. "Necessary for the performance of a task carried out in the public interest or in the exercise of official authority"[4] will, in the majority of cases, be the most appropriate lawful basis for the handling of personal data for research purposes. If you are collecting special category data as defined within the GDPR then the lawful basis for handling personal data for research purposes is public task in the public interest and in addition for scientific or historical research purposes. It is important to note that reliance upon the public task lawful basis, and the need for processing for the performance of a task carried out in the public interest, "does not automatically mean that the requirements of the common law duty of confidentiality have been met. The requirements of data protection legislation apply alongside the requirements of the common law duty of confidence: both must be satisfied'[5] and this should not conflict with ethical requirements for research studies.

The use of 'opt out' approaches in respect of research participation will still be subject to Ethics approval and should not be confused with the legal basis on which we can use the data itself. It is important not to confuse consent sought for other purposes e.g. an ethical or common law requirement, with the lawful basis for processing under data protection legislation.

Participants should be advised of the right to withdraw from a research study as before, and in addition to this have the lawful basis for retaining data collected during the study explained clearly to them, along with their right to object.

[3] General Data Protection Regulation (EU) 2016/679 Recital 33
[4] General Data Protection Regulation (EU) 2016/679 Art 6 (1) (e)
[5] NHRA Lawful Basis for Health Research v1.0 19 Dec 2017

Why would we not be processing participant data on a consent basis?

Using consent as the *lawful basis under data protection law* has ramifications that could be detrimental to research activities.

If processing of personal data in research relies on consent, it must be able to be *easily withdrawn at any point*. This is different from withdrawing from the study itself which is a right dictated by ethical practices. Withdrawing consent for the further use of personal data could mean individual participant data must be removed from stages of analysis, i.e. if that consent is withdrawn, you will **have to delete the data**, and will have no **lawful basis for retaining it** regardless of how detrimental this would be to the research involved.

There are also implications of relying on consent for data use when considering rights that individuals have under data protection law (see Data Subject Rights section below for more information). Participants will still have a legal 'right to object' to their data being held or further used for public task purposes. If we are able to delete data without detriment and there is no public or legitimate interest in refusing such a request, then we must do this. However, if we do have grounds to retain the data, then we will need to explain the reasoning; this is likely to involve your Data Protection Officer and as such requests will need to be routed through your Information Compliance team (IMPS).

Use of personal data within research activities is subject to safeguards and additional requirements at all times to protect the fundamental rights and freedoms of the research participants. These include measures to ensure that participants are clear on how the data will be used, who it may be shared with, ensuring the confidentiality, security, and integrity of the data, as well as having robust processes for minimising the use of personal data and not retaining it beyond legitimate need. These are covered in the sections below.

More guidance on how to communicate the lawful basis for the use of research data can be found within **Appendix B.**

When might we rely on consent as our lawful basis for data use?

Where participant data is collected for purposes other than the research study in question, consent may be required. An example would be where participants are also asked if they agree to be added to a register of participants who are willing to be contacted about *future* studies or to invite them to University events. You will also need consent if you plan to use the details to contact participants for marketing purposes, for example advertising school events, promoting courses or employment opportunities at the University, or for purposes other than those directly relating to the study in hand.

These additional purposes must be separated on the participant consent form to allow the participant to consent to these *separately*. This is to ensure that the consent is freely given, specific, informed and by way of an affirmative act not tied into agreeing to take part in the research study.

Should a participant change their mind about being held on a register or marketing list they will be able to withdraw their consent, and should be removed from lists used for those purposes as soon as possible.

More guidance on how to account for this in participant consent forms can be found in **Appendix C**.

If you recruit or communicate with research participants through email you should be aware that their email address may contain their personal information and the content and context of the email could reveal further personal information by the nature of the research. To avoid unauthorised disclosures of personal information the BCC function for emails should be used where appropriate.

ADEQUATE, RELEVANT, NOT EXCESSIVE (PRINCIPLE 3)

Do you need to collect personal data?

When planning your research consider whether you need to know the identity of your research participants. If it is not necessary to collect personal data, and your research can be done without collecting any personally identifiable information, you will hold anonymous data only (see further information in anonymisation) and the laws governing personal data (the GDPR) will not apply.

How much personal data do you need?

If you do need to collect personal data, you should only collect personal data where it is necessary for the purposes of your research. This data must be "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"[6].

You should also consider how specific your personal data needs to be. If you are collecting people's ages as part of your research consider whether you could ask for an age bracket, their age in years, or their date of birth. Asking for an age bracket or age in years will mean less personal data is collected. Only ask for specific dates of birth where they are vital to your study and be prepared to evidence this if asked. Similar considerations should be given to addresses, where partial addresses could be used instead. Where you are interested in specific physical or mental conditions, consider whether a higher level category could be presented as a choice, rather than a free text box that encourages a more detailed disclosure by the participant. Give due regard to data minimisation principles when utilising free text boxes for participant responses. These may encourage over sharing of personal information and selected fields of drop downs may be a method of avoiding this.

Know your objectives and purposes for the data in advance

Have your purposes for collecting any personal data clearly set out before you begin collection. You should not collect superfluous personal data on the assumption that you may find a need for it later.

Avoid unnecessary duplication of personal data

If you need to make copies, ensure that these are also deleted or minimised and that superfluous copies are deleted.

ACCURATE AND UP TO DATE (PRINCIPLE 4)

Personal data must be "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".[7]

Researchers should take care to check that the data obtained from a research participant is correctly recorded. It is also worth noting that we cannot be held accountable for inaccurate data given to us by the participants themselves, for example a misspelt name, address or email, but should the participant later inform us of an error, this must be rectified as soon as possible.

It is also important to note that data can be considered accurate at the time it was recorded, or as a historical record of events. For example, if we have a record of a previous address, this is not necessarily inaccurate, but a record of the information obtained at that time. A current address marked 'current' does not necessarily mean that the previous address needs to be deleted, providing we have a legitimate reason to retain it.

[6] General Data Protection Regulation (EU) 2016/679 Art 5(e)
[7] General Data Protection Regulation (EU) 2016/679 Art 5 (1) (d)

Where correcting inaccurate data is technically challenging it may suffice to add an annotation or note to the record to make it clear that we have received a correction and to record this somewhere it can be easily visible to those that need to view it for the purposes.

Take extra care when recording contact details, in particular email addresses, to avoid risks of sending sensitive information to the wrong recipient (bearing in mind that a mere association with a particular research project could in itself be sensitive information).

IDENTIFIABLE DATA MINIMISATION (PRINCIPLE 5)

This means you will need to collect only the minimum of personal data to begin with and wherever possible, remove the personally identifiable data when it no longer serves a purpose. One example of this would be assigning a unique reference to each participant (a pseudonym) and once all the necessary data is gathered, deleting the identifiable information collected for each participant. Once this is done, the pseudonym ID serves to differentiate each participant from the others but cannot be used to identify any participant in the working dataset. Keeping the pseudonymised working data separate from the data that matches it to participants is one example of a data minimisation technique.

Anonymisation and pseudonymisation

Anonymous data is not subject to data protection laws such as the GDPR. Pseudonymised data is, and remains personal data.

'Anonymised' in data protection law terms means that the data cannot be matched to a participant by anyone. This includes the researcher, anyone working with the data, any hosting tools used to collect the data, and anyone the data is shared with.

'Pseudonymised' means we may have applied a 'key' or unique reference to a participant but we (or someone else) are still able to match that reference back to an individual. If we share data that has been pseudonymised with another party, and they cannot identify who it relates to, it will still fall under the definition of personal data for as long as anyone can match it to an individual and will therefore remain subject to data protection laws.

Avoid using the phrases 'your answers will be anonymous' or 'your data will be held anonymously' if you will be collecting or holding personal data, whether directly, or in pseudonymised form. Only use these phrases where the data will be truly anonymised (see above).

Instead let participants know that their data will be held 'securely and in confidence'. You may want to communicate who will have access and that this is limited to several researchers or a specific team or department (however, this is not a requirement of the data protection laws).

As you will need to meet the data minimisation principle, explain that their identifying personal data will only be held for as long as it is necessary to complete the research study. Explain who the personal data may be shared with externally (see Data Sharing section below) and if applicable, that this will only be shared 'in a format that will not identify you to the other party' (pseudonymised) and 'only where agreements are in place to protect the data and keep it secure'.

If you are then going to retain *truly anonymous* or aggregated data, you can retain this indefinitely providing that it does not relate to any identifiable individuals. You do not need participant consent to retain or share truly anonymous data but you may wish to include details of what anonymous data is used for in your information sheet if you feel it would benefit the participant.

Data protection laws are no barrier to the sharing of *anonymised* research data, whether in institutional repositories, research publications or otherwise. If unsure, seek advice from the University Data Protection Officer.

More information on anonymisation can be found in the Information Commissioner's guidance

https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/

RECORD RETENTION

Personal data must be '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'.[8]

This means that that you will need to consider at what point the personal identifying data of your participants can be anonymised. This should be the point at which you no longer need to retain personal details for a legitimate purpose and at this point, all personal identifying data should be deleted. In some cases you may have a legitimate reason to retain participant personal data for longer periods, for example for studies that require follow ups or comparative studies at later intervals. Where this is the case, this should be explained to the participants at the outset. Where personal data is retained, data minimisation principles apply (see Data Minimisation).

Prescriptive retention periods for *'all research data'* are not required for the purposes of data protection compliance and may be detrimental to the ability to use research outputs for future legitimate purposes. Assurances that ALL research data will be destroyed after a specified number of years are not necessary and should be avoided. Instead, participants should be informed of the measures that will be taken to *minimise the amounts of personal data* being used during the research study, and advised of an indicative maximum time that the personally identifiable information will be stored for these purposes (remember this will include any pseudonymised data).

Example wording for information sheets can be found in Appendix C.

You will be responsible for ensuring that data is stored in a manner that enables retention and deletion to be effectively managed if you depart the University.

Retention exceptions for personal data used for research purposes

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[9]. This means where you have legitimate and evidenced reasons for retaining personal data for longer, you can lawfully do so; but this can only be done where you have appropriate safeguards in place to protect it (such as data minimisation and adequate security protections) and providing that you identified a point at which retention of that data will be reviewed (a retention schedule or plan for example).

SECURITY (PRINCIPLE 6)

It is vitally important that research data containing personally identifiable information is collected, held, shared and disposed of securely. Access to research data should be limited to a strictly need to know basis. If you are storing research data on University property or within the University IT estate, ensure that you have considered who can access the data and how it can be disposed of or deleted when no longer needed.

If you are working on a personal device you must follow the University Information Security Policies: http://www.reading.ac.uk/internal/imps/policiesdocs/imps-policies.aspx

[8] General Data Protection Regulation (EU) 2016/679 Art 5 (e)
[9] General Data Protection Regulation (EU) 2016/679 Art 5(e)

IT have guidance on accessing your files through the Virtual Private Network (VPN) here: http://www.reading.ac.uk/internal/its/help/its-help-networks/its-network-vpnfaq-old.aspx

DATA SHARING

Where personal data is shared with individuals, companies, institutions or any other third parties to the University it will constitute a disclosure of the information from the University to another party.

We have a responsibility to ensure that personal data is shared securely and only with those who can evidence that they will also handle the data in line with all the above data protection principles.

Contractual clauses of terms within contracts and/or information sharing agreements with collaborators or other third parties receiving personal data are ways in which this necessary due diligence can be evidenced and should always be put in place. These agreements serve to ensure that all parties are clear on what their respective obligations and responsibilities for data protection are.

If you are sharing personal data for research purposes and need advice consult with the University Data Protection Officer and the Research Enterprise Services team.

More information on the statutory code of practice for information sharing, issued by the Information Commissioner's Office can be found here (subject to awaited updates following GDPR implementation):

https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/

RESEARCH SURVEY TOOLS

In many cases, an external supplier providing a tool for the collection of personal data will be act as 'data processor'. In simple terms this means that the University (as the 'Data Controller') decides the purposes for the data collection, and the supplier (as the Data Processor) provides the means for processing that data on our instruction.

Under data protection law we are required to only use suppliers providing "sufficient guarantees to implement appropriate technical and organisational measures [...] and ensure the protection of the rights of the data subject"[10]

When you use an externally hosted tool for conducting research surveys or questionnaires, the University will in many cases remain responsible for ensuring the provider of that tool is meeting all obligations in respect of security and data protection compliance. Before using any third party to handle personal data for our purposes we must ensure:

- We have conducted necessary due diligence on the security and data protection measures of that provider. This can include requesting evidence of staff training, policies and procedures, technical security, how the data will be stored, shared and disposed of, and necessary limitations on further use.

- We have written terms in place with that provider that include how they will keep information secure, that the data will not be used for any other purposes without consent, that the data will remain under the control of the University and not be retained beyond our instructed use, and that the supplier will assist with security incidents and data subject access requests. All such contractual terms should be reviewed by procurement or Legal Services (as appropriate).

If you are collecting data via an online or digital survey tool you will still need to provide participants with a privacy notice before they begin the survey.

[10] General Data Protection Regulation (EU) 2016/679 Art 28 (1)

You will need to establish how the data will be handled after the survey is completed and the data has been extracted. How can it be deleted from the survey tool platform? Is it your responsibility to do this or is there a default delete after a set period of time?

Commonly used research survey tools are Online Surveys, Qualtrics, and Survey Monkey. If you have a query about using an online research survey tool please contact IMPS.

DATA SUBJECT RIGHTS

Individuals have certain rights under data protection laws. These are listed below:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

There are exemptions from some of these rights where personal data is used for the purposes of research. Many of the requests made in exercise of these rights must be responded to within 1 month. If you receive a request from a participant to exercise a right under the GDPR or other data protection laws, please consult with your Data Protection Officer via imps@reading.ac.uk as soon as possible.

CONTACTS AND RESOURCES

Information Management and Policy Services

imps@reading.ac.uk 0118 378 8991

For advice on data protection laws and requirements and to contact the University Data Protection Officer

University Research Ethics Committee

urec@reading.ac.uk

Research Data Management

researchdata@reading.ac.uk **0118 378 6161**

Information Commissioners Office

https://ico.org.uk/

Code of practice on anonymisation

https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/

GDPR guidance on consent

https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

MRC *Good practice principles* Appendices 2 and 3 (http://www.methodologyhubs.mrc.ac.uk/files/7114/3682/3831/Datasharingguidance2015.pdf, p. 23-28);

Hrynaszkiewicz I et al. (2010), 'Preparing raw clinical data for publication: guidance for journal editors, authors, and peer reviewers'. British Medical Journal 340:c181. https://doi.org/10.1136/bmj.c181;

UK Data Service: Anonymisation (https://www.ukdataservice.ac.uk/manage-data/legal-ethical/anonymisation).

Version control

VERSION	KEEPER	REVIEWED	APPROVED BY	APPROVAL DATE
1.0	IMPS	6 Monthly	IMPS/GDPR Research Group	May 18

APPENDIX A: CHECKLIST FOR RESEARCHERS

Data Protection checklist for Researchers

Contents

Introduction

This Checklist is for use by anyone who is planning to undertake research that will involve the collection of personal data from researchers. It consists of 9 things that you should do before you start your research.

The Checklist is a planning tool, and can be used as to inform your data management plan. A comprehensive guide to Data Protection for Researchers is available from the IMPS website at http://www.reading.ac.uk/imps-d-p-dataprotectionandresearch.aspx.

1. Specify the purpose or purposes for which you require the personal data

The purpose(s) for which personal data are required must be stated in the privacy notice supplied to research participants. If you plan to process the data for any purpose other than the proposed

research, this should be clearly defined. For example, consider whether you will want to establish a database of potential participants in future research. In such a case, you would need to secure separate consent, aside from consent given for participation in the research.

2. Identify who will have access to the personal data

Access to personal data should always be on a need-to-know basis. In many cases, not all members of a research team will need to know the identities of the research participants. Participant information and linked pseudonyms can be stored in a separate online or physical location accessible by an authorised group only, e.g. the PI and Co-I, while a pseudonymised or anonymised version of the data could be made accessible to other members of the team for analysis.

If the personal data will be collected by or shared with contractors or partners outside of the University, identify these. These parties will be either Data Controllers or Data Processors.

3. Identify the Data Controllers and the Data Processors

Who determines the purposes and the manner of data processing? Who will process the personal data on behalf of the Data Controller?

If University staff or students working for or under the instruction of the University will determine the purpose and manner of processing, the University will be the Data Controller.

If project partners will process personal data under instruction from University members, they will be Data Processors.

Project partners may also determine the purposes and/or manner of personal data processing, in which case there will be more than one Data Controller.

Data Processers might be organisations conducting data collection on the University's behalf, or the providers of instruments used for data collection, e.g. online survey tools.

Any disclosure of data outside the University should take place under a contract in which the data protection responsibilities of other parties are defined. For example, where the joint Data Controller or Data Processor is a partner in a project, data protection responsibilities should be written into the research collaboration agreement. Where the Data Processor is a contractor, data protection responsibilities should be included in the service contract.

- Contact Research Contracts for advice on collaboration agreements.
- Contact IMPS or Legal Services for advice on service contracts.

4. Specify the personal data you will need to collect

Consider the nature of the information you will collect from the research participants, and in particular whether any of it, when combined with their personal information, falls into the special categories of data as defined under the GDPR. Special category data includes information about an individual's race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation. Any personal data falling into these categories should be identified and will need to be managed with extra care.

For example, opinions of identifiable members of the public about building design are unlikely to fall within a special category of data; the mental health history of identifiable adolescents with anxiety and depression falls within the special category of data concerned with an individual's health.

Consider also what personally-identifying information you will or may collect. You should collect only the minimum necessary for your purposes. For example, for participation in an observational study, you

might collect the person's name, address, email address and telephone number, to facilitate contact; for an online screening survey, you may need only to collect an email address.

Bear in mind that qualitative data collection, for example, by means of interview, observation, photography, and creative expression by participants, may yield personally-identifying references incidentally, even if interviews are conducted 'anonymously'.

5. Decide whether you will need to conduct a Data Protection Impact Assessment

You are required to carry out a Data Protection Impact Assessment (DPIA) if your processing of personal data is likely to result in a high risk to individual's interests. High risk could result from either a high probability of some harm, or a lower possibility of serious harm. Some examples of high risk data processing include processing special category data on a large scale, processing biometric or genetic data, and processing personal data in a way which involves tracking individuals' online or offline location or behaviour.

The purpose of a DPIA is to:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

If a DPIA is required, this must be carried out with the involvement of the University's Data Protection Officer.

To find out whether you need to conduct a DPIA, you should read the University's Data Protection Impact Assessment guidance, and assess your proposed personal data processing against the DPIA Screening Checklist. The guidance and checklist can be found at http://www.reading.ac.uk/imps-d-p-dataprotectionbydesign.aspx.

Please send your completed DPIA Screening Checklist to the University's Data Protection Officer at imps@reading.ac.uk. The Data Protection Officer will then assist you in conducting a DPIA.

6. Specify the means by which the information will be collected and stored

Information is likely to be collected and stored using different media. Map your data workflow, and identify measures for securing the personal data in its holding locations and in transit between them.

Security controls such as password protection access controls can be applied to individual files, folders, storage volumes, and devices. It is advisable to use some level of access control for all digital personal data holdings, and to use encryption to protect sensitive data.

Digital channels of communication can be encrypted, so that only the sender and receiver can read the message. The University VPN provides a secure connection to the University network. If you are collecting data via online survey tools you should check that data are securely protected when transferred to and from the service provider. Email messages are not encrypted by default, and should not be used to send unprotected files containing large volumes of personal data or sensitive data. The University Encryption Policy (which can be downloaded from http://www.reading.ac.uk/imps-policies.aspx) defines requirements for the use of encryption for sending data outside the University network.

IMPS provides guidance on encryption on its web pages. IT can advise on managing access permissions to fileshares and folders on the University network.

Be especially careful when using cloud services for the storage and transfer of personal data. University OneDrive accounts are suitable for storing personal data, although care should be taken to share such data with nominated authorised recipients only.

Other cloud services (such as Dropbox, Google Drive, iCloud, etc.) are not underwritten by any institutional guarantees, and their terms of service may offer inadequate protection for personal data. For example, if data held in cloud services are stored on servers in countries outside the European Economic Area, and an equivalent level of protection for personal data is not provided in a these countries, researchers using these services to store personal data risk being in breach of data protection laws. If you are in doubt about the compliance of any cloud service with data protection laws, you should consult IMPS or IT for advice.

Here are two examples of approaches to protecting data throughout the research workflow:

Example 1

Interviews will be recorded on a password-protected audio recording device. Recordings will be transferred by encrypted VPN connection to an access-controlled folder in a fileshare managed by the PI on the University network. Once transfer is verified, recordings will be wiped from the audio device. A member of the project team will produce anonymised transcripts of the audio recordings, using their campus PC and saving all materials to the same network location.

Example 2

Screening data for an observational study, including information about an individual's health, will be collected by means of the Online surveys tool. Online surveys provides end-to-end encryption of survey responses. Data held by Online surveys will be stored on servers based in Ireland, in the European Economic Area. Data will be exported from Online surveys via encrypted connection to Excel and will be stored in the PI's University OneDrive account. Once data have been exported, they will be deleted from BOS.

For selected participants, participant information and signed consent forms will be collected on paper in private rooms at the on-campus clinic, and will be stored in a locked filing cabinet in the PI's office. Participant information will be input into the study database by the Research Assistant. Consent forms will be digitised, and stored with participant information in a restricted folder, accessible by the PI only, within the project fileshare on the University network. Paper forms will be destroyed once they have been digitised and saved. Participants will be assigned a unique identifier, which will be recorded in the restricted folder against the participant information. For the research experiments, participants will be identified by their unique identifier only. Results of laboratory-based tests will be recorded in an Excel file against the participant's unique identifier and saved to an area of the fileshare accessible to all members of the project team.

Consider also that personal data may be held in different locations during the project and for the longer term after the project.

- Contact IT for guidance on suitable University-managed services for the storage and transfer of personal data, and assistance with encryption and access controls.
- Contact IMPS or IT for advice on suitable cloud services for storage and transfer of personal data.
- Contact your School or Department administrator if you need somewhere secure to store paper-based personal data.

7. Anticipate how long the personal data will be retained

Personal data should not be retained longer than necessary, but may be retained beyond the duration of the original research project if they are held for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes. For example, if follow-up studies are

contemplated, then continued retention is justified, providing this purpose has been notified to the individual.

If the only purpose for which data are being collected is to undertake a given study, then personal data should not be retained longer than necessary to complete the research and publish the results. Consent forms provide an auditable record of informed participation in the research, and you should take into account any contractual, legal, or statutory obligations that are specific to your study when deciding how long to retain them; as a minimum they must be retained for as long as any personal data collected from the participants is held by the University.

Care should be taken to avoid commitments to destroy personal data by a given time, e.g. 3 years after the completion of the project. It is better to schedule regular reviews of personal data holdings to determine whether they need to be retained or can be safely destroyed.

If personal data will be retained in the long term after the completion of the research, planning should take into consideration where and under whose authority they will be held, and what provision is made for transfer of ownership should the original owner leave. For example, a research group could maintain a personal data asset register, listing personal data held, owners of the data, their storage locations, the retention schedule, and the date of next review. This register could then be updated on an annual basis and ad hoc when a review date is reached, or when any listed data owner leaves the University.

8. Plan for pseudonymisation and anonymisation of personal data

To minimise the risk of inappropriate disclosure of personal data, it is advisable to create pseudonymised or, where possible, anonymised versions of working data. Data can often be pseudonymised for purposes of processing and analysis, with the personally-identifying information and their linked pseudonym IDs stored separately from a dataset in which individual identifiers have been replaced by the pseudonym IDs.

This may be a first step towards full anonymisation of the data. Bear in mind that the University and many funders require data supporting research findings to be preserved and made publicly available on publication of results wherever possible,[11] so it will in any case be necessary to prepare an anonymised version of the data towards the completion of research.

In the case of pseudonymised data, they will continue to be personal data as long as the identifying 'key' data is held, whether by the University or a third party. But using pseudonymisation is one way to minimise the risks of any data subjects being identified if data is shared with another person or organisation that does not have any access to the identifying data.

In one-off study scenarios it is often appropriate to destroy the linking key when the study is completed, so that data become fully anonymised. In some cases, for example where participants have been recruited for longitudinal studies, there may be a need to retain the key while anonymised versions of data are created for public release.

Bear in mind that effective anonymisation may involve much more than replacing personal names with pseudonyms, and different techniques are required for quantitative and qualitative data.

Some data collected from research participants may be difficult or impossible to anonymise effectively. Examples include: photographic images and video recordings featuring individuals, personally identifiable genetic and phenotypic data, and biometric information used for identification purposes. Where the information falls within a special category of data, extra care will need to be taken in their collection, storage and disclosure. Managed disclosure of such data in support of published results may still be possible: data archiving services such as the UK Data Service and the European Genome-

[11] The University's Research Data Management Policy is available at http://www.reading.ac.uk/reas-RDMpolicies.aspx.

phenome Archive[12] can manage controlled access to confidential data collected for research purposes. If you do plan to collect inherently confidential data, you should seek consent for controlled sharing and include in the consent form a statement such as this:

'I understand that the data collected from me in this study will be preserved, and will be made available to other authenticated researchers only if they agree to maintain the confidentiality of the information provided to them.'

- Contact the Research Data Manager for advice on planning for data sharing.

Guidance on anonymisation techniques

MRC *Good practice principles* Appendices 2 and 3 (p. 23-28).
http://www.methodologyhubs.mrc.ac.uk/files/7114/3682/3831/Datasharingguidance2015.pdf

Hrynaszkiewicz I et al. (2010), 'Preparing raw clinical data for publication: guidance for journal editors, authors, and peer reviewers'. British Medical Journal 340:c181. https://doi.org/10.1136/bmj.c181

UK Data Service: Anonymisation. https://www.ukdataservice.ac.uk/manage-data/legal-ethical/anonymisation

9. Prepare the information sheet and consent form

The consent form provides documented evidence that the research participants have received the privacy notice and are aware of the lawful basis, purpose(s) and manner of data processing. Take care not to prejudice your research by poorly formulated information sheets and consent forms. In particular make sure that the purposes for which the data are being collected are clear, but do not place unnecessary restrictions on your use of the data, and notify participants if you plan to retain personal data for purposes other than those of the original research.

Make sure that the privacy notice includes the following:

- The name and contact details of the Data Controller(s) and the contact details of the Data Protection Officer;
- The purpose(s) for which the personal data are being collected;
- The lawful basis for processing the personal data;
- The categories of personal data to be collected;
- The recipients of the personal data, including third parties the data may be shared with;
- The details of the transfer of the personal data to any third countries or international organisations (if applicable);
- The retention periods for the personal data;
- The rights available to individuals in respect of their personal data, including the right to withdraw consent;
- The right to lodge a complaint, i.e. with the ICO;
- The source of the personal data (if not obtained from the individual);
- Details of the existence of automated decision-making, including profiling (if applicable).

- Contact IMPS for guidance on privacy notices.
- Contact Research Ethics or the Research Data Manager for guidance on consent forms.

[12] UK Data Service: https://www.ukdataservice.ac.uk/deposit-data/preparing-data/confidential-data; European Genome-phenome Archive: https://www.ebi.ac.uk/ega/home.

Guidance on information/consent and sample information sheets and consent forms

University sample information sheet and consent form. http://www.reading.ac.uk/imps-d-p-dataprotectionandresearch.aspx

University Research Ethics Guidance Notes with sample information sheet and consent form. http://www.reading.ac.uk/internal/academic-and-governance-services/research-ethics/RECethicshomepage.aspx

UK Data Service: Consent for data sharing. https://www.ukdataservice.ac.uk/manage-data/legal-ethical/consent-data-sharing

Contacts

Team	Advises on	Email	Tel.
IMPS	Compliance with data protection law; privacy notices; encryption policy	imps@reading.ac.uk	0118 378 8981
IT	Services for storage and transfer of digital data; using encryption and access controls for data	it@reading.ac.uk	0118 378 6262
Legal Services	Service contracts with data processors	legalservices@reading.ac.uk	0118 378 6742
Research Contracts	Collaboration and partnership agreements	res@reading.ac.uk	0118 378 8628
Research Data Manager	Planning and consent for data sharing; preparing participant-derived data for public release	researchdata@reading.ac.uk	0118 378 6161
University Research Ethics Committee	Use of confidential data in research; ethical approval process; information sheets and consent forms	urec@reading.ac.uk	0118 378 7119

APPENDIX B: SAMPLE CONSENT FORM

Remove any statements that are not applicable and guidance notes

Consent Form

Please use tick box after each statement to confirm it has been read and agreed to.

1. I have read and had explained to me by ..... the accompanying Information Sheet relating to the project on: .....

2. I have had explained to me the purposes of the project and what will be required of me, and any questions I have had have been answered to my satisfaction. I agree to the arrangements described in the Information Sheet in so far as they relate to my participation. ☐

3. I have had explained to me what information will be collected about me, what it will be used for, who it may be shared with, how it will be kept safe, and my rights in relation to my data. ☐

4. I understand that participation is entirely voluntary and that I have the right to withdraw from the project any time, and that this will be without detriment. ☐

5 (a). I understand that the data collected from me in this study will be preserved and made available in anonymised form, so that they can be consulted and re-used by others. ☐

5 (b). I understand that the data collected from me in this study will be preserved, and subject to safeguards will be made available to other authenticated researchers. ☐ *

(*Guidance note only safeguards will include pseudonymisation, data minimisation, secure transfers, and any necessary data sharing and confidentiality agreements between parties)

7. I authorise the Investigator to a) consult my General Practitioner. b) I authorise my General Practitioner to disclose any information which may be relevant to my proposed participation in the project. ☐**

(**Guidance note only - If applicable Researcher to delete (a) and (b) if GP will not be contacted, or (b) if no response from GP is required a))

8. This project has been reviewed by the University Research Ethics Committee and National Research Ethics committee where relevant, and has been given a favourable ethical opinion for conduct.

9. I have received a copy of this Consent Form and of the accompanying Information Sheet. ☐

Name: .....

Date of birth: .....

Signed: .....

Date: .....

I am happy to be included on a register of research participants for the purposes of being contacted about further studies by..... Please tick ☐ (optional)

APPENDIX C: DATA PROTECTION FOR INFORMATION SHEETS

To be added to all participant information sheets. Please note, if you are providing this information to children, or individuals that may need more simple terms to help them understand this information please amend to suit your audience. If you need advice please contact imps@reading.ac.uk

The organisation responsible for protection of your personal information is the University of Reading (the Data Controller). Queries regarding data protection and your rights should be directed to the University Data Protection Officer at imps@reading.ac.uk, or in writing to: Information Management & Policy Services, University of Reading, Whiteknights, P O Box 217, Reading, RG6 6AH.

The University of Reading collects, analyses, uses, shares and retains personal data for the purposes of research in the public interest. Under data protection law we are required to inform you that this use of the personal data we may hold about you is on the lawful basis of being a public task in the public interest and where it is necessary for scientific or historical research purposes. If you withdraw from a research study, which processes your personal data, dependant on the stage of withdrawal, we may still rely on this lawful basis to continue using your data if your withdrawal would be of significant detriment to the research study aims. We will always have in place appropriate safeguards to protect your personal data.

If we have included any additional requests for use of your data, for example adding you to a registration list for the purposes of inviting you to take part in future studies, this will be done only with your consent where you have provided it to us and should you wish to be removed from the register at a later date, you should contact.....

You have certain rights under data protection law which are:

- Withdraw your consent, for example if you opted in to be added to a participant register
- Access your personal data or ask for a copy
- Rectify inaccuracies in personal data that we hold about you
- Be forgotten, that is your details to be removed from systems that we use to process your personal data
- Restrict uses of your data
- Object to uses of your data, for example retention after you have withdrawn from a study

Some restrictions apply to the above rights where data is collected and used for research purposes.

You can find out more about your rights on the website of the Information Commissioners Office (ICO) at https://ico.org.uk

You also have a right to complain the ICO if you are unhappy with how your data has been handled. Please contact the University Data Protection Officer in the first instance.

Below information to be added unless covered in other areas of the Information Sheet (see guidance for what needs to be included)

The purposes of the use of personal data (what the study is for)

The categories of personal data that are not obtained directly from the participant (if applicable)

The recipients or categories of recipients of the personal data (to include third parties the data may be shared with, for example, other researcher at HEI's, organisation or job role)

The details of transfers of the personal data to any countries outside the EU including international organisations (if applicable).

The retention periods for the personal data.

The details of the existence of automated decision-making, including profiling (if applicable – more information on whether this would apply to your study can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/