The EU GDPR 2016 is the law that sets out the requirements for the protection of personal data within the EU. Following the UK's departure from the EU, from the 1st January 2021, the requirements of the EU GDPR were adopted into UK laws, creating the 'UK GDPR'. The EU GDPR will remain relevant to data collected and processed prior to the 31st December 2020 and to the data of EU residents from there

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.

**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If processing of personal data in research relies on consent, it must be able to be *easily withdrawn at any point*.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personal data could mean individual participant data must be removed from stages of analysis, i.e. if that consent is withdrawn, you will **have to delete the data**, and will have no **lawful basis for retaining it** regardless of how detrimental this would be to the research involved.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.**

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.

### 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].

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.

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).

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.

*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

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/media/for-organisations/documents/1061/anonymisation-code.pdf

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



82 8 of 125 Tc 0.915 200 0 8 Tw 2 Tr 0.T1 0 0 1 812(re v)-o0 1 b6 rpti7 477. 0 1 812(re vil)1ET-3(of)11TBT( )-3(for e )8(s)-4on nohe3( )T

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

- 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.

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.

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.

Code of practice on anonymisation

https://ico.org.uk/media/for -organisations/documents/1061/anonymisation -code.pdf

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 | KEEPER |
|---|---|

# Data Protection checklist for Researchers

## Contents

Introduction ..... 11
1. Specify the purpose or purposes for which you require the personal data ..... 11
2. Identify who will have access to the personal data ..... 11
3. Identify the Data Controllers and the Data Processors ..... 12
4. Specify the personal data you will need to collect ..... 12
5. Decide whether you will need to conduct a Data Protection Impact Assessment ..... 12
6. Specify the means by which the information will be collected and stored ..... 13
7. Anticipate how long the personal data will be retained ..... 14
8. Plan for pseudonymisation and anonymisation of personal data ..... 15
9. Prepare the information sheet and consent form ..... 16
Contacts ..... 17

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.

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.

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.

©University of Reading

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.

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 instiny

*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*

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

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

The consent form provides documented evidence that the research participants have received the

**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: University of Reading, Information Management & Policy Services, Whiteknights House, Pepper Lane, Whiteknights, Reading , RG6 6UR, UK.

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/