Data Protection & Research

Introduction

Research projects undertaken at the University will often involve information relating to individuals. This information must be processed in accordance with the requirements of data protection law.

The purpose of this note is to introduce researchers to the provisions of the following legislation on data protection:

General Data Protection Regulation (GDPR)

The GDPR is an EU Regulation that applies directly to the UK while it remains a member of the EU. The UK government has indicated that the requirements of the GDPR will be incorporated into UK law when the UK ceases to be a member of the EU.

Data Protection Bill/Data Protection Act 2018

The Data Protection Bill, which is currently before Parliament, will supplement the GDPR by legislating in those areas where Member States have discretion to vary or adapt GDPR provisions. A number of its clauses relate specifically to research.

This note focuses mainly on the GDPR, as it is the more significant piece of legislation. References to the GDPR should be taken to mean the GDPR, as supplemented by the Data Protection Bill. The note will be updated after the Data Protection Bill has been finalised and formally enacted.

The implications of the GDPR for research will be explained with particular reference to the following questions and issues:

Researchers may need further guidance, particularly in applying legal requirements to specific projects. This is available from the University's Information Compliance Team and from the Legal Services Office.

It should be noted that the University has prepared a suite of templates which can be adapted for use by researchers collecting and sharing information about individuals. For further information about these templates, please contact Research Services.

A. What is data protection?

In policy terms, data protection law aims to strike a balance between: (a) the privacy interests of individuals, and, (b) the needs of organisations to make fair and reasonable use of information relating to those individuals in their operations. It does *not* mean that researchers cannot make use of such information, or that they must always have an individual's consent to do so, but it does impose controls and restrictions which must be complied with.

Technology has made it possible to collect and use increasing amounts of information about individuals in ever more diverse ways. The GDPR will introduce a new framework to safeguard the rights of those individuals.

B. Why is data protection important?

Compliance with the GDPR is a legal requirement. Breaches of data protection law may result in investigations, significant fines, adverse publicity, and civil or criminal liability. Enforcement action may be taken by the Information Commissioner's Office (the "**ICO**"), which has the power to issue fines or require changes in an organisation's policies and procedures. If the University fails to comply with its legal obligations, such an action could be taken against the University and published on the ICO's website, resulting in reputational damage. Individuals have extensive rights under the GDPR, which they may exercise by submitting requests to organisations using their data (see section H for further information). If they are dissatisfied with the University's response, they may complain to the ICO. Individuals may also bring legal claims for damage or distress.

More generally, the University is committed to responsible processing of information relating to individuals and to respecting their rights to data privacy. Although the consideration of data protection law may seem like an additional burden, much of it is plain common sense and, indeed, oftentimes consistent with the ethical requirements of many research projects.

C. Does your project involve information to which the GDPR applies?

The GDPR only applies to the "**processing**" of "**personal data**". It will usually be obvious whether your project falls within the scope of the GDPR, but this may not always be the case and the constituent elements of this phrase are considered below.

1. Are you processing?

Processing means almost anything a research team might do with personal data, including: collecting it; holding or storing it; retrieving, consulting or using it; organising or adapting it; publishing, disclosing or sharing it; and even destroying it.

2. Does your project involve personal data?

Personal data is information which relates to a living individual who can be identified from that information, whether directly or indirectly, and in particular by reference to an identifier. It includes, for example, a name, an identification number, location data, or an online identifier, such as the IP address, as long as that information can be linked by the University to a living individual. It could also include information that identifies an individual's characteristics, whether physical, physiological, genetic, cultural or social.

This definition is intentionally broad, and its application to particular types of research data is considered in more detail below. Where there is any doubt, the ICO advises erring on the side of caution with regard to the interpretation of personal data and looking to the flexibility in the application of the data protection principles (see sections F and G below).

Anonymous data

The ability to identify the individual to whom the information relates is crucial to the definition of personal data. Where that individual cannot be identified, and it is not possible to re-identify the individual, the information will not constitute personal data and the duties and obligations of the GDPR will not apply.

Researchers should, however, consider whether or not an individual is identifiable, notwithstanding the removal of the usual identifiers. Indeed a combination of details on a categorical level (e.g. age, regional origin, medical condition, etc.) may allow an individual to be recognised by narrowing down the group to which they belong.

In determining whether an individual is identifiable, account should be taken of all the means reasonably likely to be used to identify that individual, whether by the research team or by any other person. While this does not include a mere hypothetical possibility, it does require consideration of the means that are likely to be used by a determined person with a particular reason to want to identify an individual.

Pseudonymous data

Pseudonymisation is the practice of disguising the identities of individuals to whom information relates. This usually involves the removal of common identifiers and the use of a pseudonym (often a randomly allocated number), so that data can be continually collected about the same individual without recording their identity. Pseudonymising data can be useful in research.

Pseudonymous data can be collected in such a way that no re-identification is possible (e.g. one-way cryptography), in which case it is essentially anonymous data and the considerations above apply. However, it is often retraceable (e.g. key-coding and two-way cryptography) and therefore may be personal data. Where the researcher (or any other person operating within the University) possesses the means to identify any of the individuals to whom the information relates, that information will still constitute personal data. Where, however, the pseudonymised data is received from or supplied to third parties without the means to identify the individuals, the effectiveness of the pseudonymisation will depend on a number of factors (e.g. how secure it is against reverse tracing, and the size of the population in which the individual is concealed).

Aggregated data

Aggregation is the process of combining information about many individuals into broad classes, groups or categories, so that it is no longer possible to distinguish information relating to those individuals. It follows that this data should not be personal data, but its effectiveness will depend on such factors as the size of the population in which the individual is concealed.

Biometric data, DNA and human tissue samples

The definition of personal data in the GDPR includes biometric data where it allows the unique identification of an individual, as well as genetic data. The term biometric data is used here to describe those intrinsic, biological, physical or behavioural traits that are both unique to an individual and measurable. Examples commonly include fingerprints, retinal patterns, facial structure, voice, hand geometry, and vein patterns; but biometric data also includes deeply ingrained skills and behaviours (e.g. a handwritten signature and a particular way of walking or speaking).

Biometric data has a dual character in that it is both information about a particular individual and information which is capable of identifying an individual. DNA shares this duality of character. Accordingly, in most cases biometric data and DNA will be personal data for the purposes of the GDPR, in which case it will also be "special category personal data" (see below).

Human tissue samples may provide a source from which biometric data can be extracted, but they are not biometric data themselves; that is, the extraction of information from samples

may result in the collection of personal data. The collection, storage and use of tissue samples are subject to different laws, except that those samples may be accompanied by information (e.g. name, age, etc.) which also constitutes personal data.

Photographs, videos and sound recordings

Where an individual participates in research which involves a recorded interview, that individual may disclose personal data about themselves or other people. However, researchers should also be aware that the existence of photographs, videos and sound recordings of people (whether or not those individuals voluntarily disclose any information) may comprise information about that individual and may allow that individual to be identified. Accordingly, these are media which are capable of being personal data).

D. What is special category personal data[1]?

The GDPR recognises that some categories of personal data are particularly private and/or could be used in a discriminatory way. As a result, the GDPR requires researchers to treat this "**special category personal data**" with greater care.

> *Special category personal data* includes any personal data consisting of the following information: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data for the purpose of uniquely identifying a person; health; sex life and sexuality.

Information about criminal convictions and offences is not included in the definition of special category personal data, but may be processed only under the control of official authority or when authorised by domestic law, which provides for appropriate safeguards. The Data Protection Bill lays down specific conditions for the processing of criminal offence data.

Due consideration should be given to information which may indirectly disclose special category personal data about an individual. For example, photographs and names may give an indication of a person's race or religious beliefs, but will not always be special category data merely because an assumption about a person's race or religious belief might be drawn from appearance or name. The issue will arise if that information is processed on the basis of those assumptions (for example, grouping people based on skin colour or likely ethnic origin of surname). The additional legal requirements in relation to special category personal data are described below (see section F).

E. Who is responsible for complying with the GDPR?

The GDPR imposes obligations on both "**data controllers**" and "**data processors**".

A data controller is the person who (either alone or jointly with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. Essentially, do you have control over how you may use the information?

The data processor is the party who does the processing of personal data on behalf of the data controller. Are you acting pursuant to someone else's instructions?

For research projects based at the University, the University will most likely be the data controller. It does not matter if the research project is taking place in a country outside the UK

[1] Special category personal data was previously known as "sensitive" personal data, which under the Data Protection Act 1998 included criminal convictions and allegations

or EEA[2], the GDPR will apply irrespective of where the data processing is taking place if the University is processing personal data or is the data controller.

You are required by your employment contract with the University to comply with the GDPR. Where the University is the data controller and you intend to supply any personal data to a third party to perform any subcontracted work, such transfer *must* be made under an appropriate contract.

Where the University and a third party are collaborating on a research project, both the University and the third party are likely to be data controllers. In this situation, an agreement should be in place between the University and the third party setting out their respective responsibilities for compliance with the GDPR. Data subjects should be able to exercise their rights under the GDPR against either of the controllers, and therefore they should be informed of the arrangements in place between the University and the third party. If you are collaborating with a third party, you should approach Research Services for guidance.

If the University is not the data controller in respect of processing of personal data (e.g. where work is being performed on behalf of another party who determines the means and purpose of processing for the University), the obligations of the GDPR will still apply to the University as a data processor. This would mean, for example, that the University would be responsible for ensuring the security of the data and for keeping records of processing activities.

F. What are your duties and obligations under the GDPR?

Data protection principles

Researchers must process all personal data in accordance with the "**data protection principles**", unless there is a relevant exemption (see section H below). There are other requirements in the GDPR, but the data protection principles represent the core requirements.

Data protection principles

Personal data must:

1. be processed lawfully, fairly and in a transparent manner;
2. be collected only for specified, explicit and legitimate purposes, and not be further processed in any manner incompatible with those;
3. be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. be accurate and, where necessary, kept up-to-date;
5. not be kept as identifiable data for longer than necessary for the purposes concerned; and
6. be processed securely.

Most of the data protection principles are self-explanatory, but they benefit from further comment in a research context.

[2] Please note that the EEA includes the 27 member states of the European Union and the European Free Trade Association states (Norway, Lichtenstein and Iceland).

1. Fair, lawful and transparent processing

This is, perhaps, the most important data protection principle: it is the overriding objective of the GDPR and all the subsequent data protection principles are, in effect, requirements for complying with this principle. There are three aspects to this data protection principle, which are discussed below.

Fair processing

'Fair' processing requires researchers to consider more generally how their use of personal data affects the interests of the individuals to whom it relates. In circumstances where your use may cause detriment to an individual, you need to consider whether or not that detriment is justified. Fairness is naturally linked also to the transparency of the processing and the ability of the individual to object.

Lawful processing

Personal data

The processing of personal data must have a lawful basis (a legally acceptable reason for processing the data), which must be documented by the data controller. Of the six possible legal bases specified in the GDPR, three are of relevance to research.

- **Public interest task** – this will likely be the most common legal basis for processing, and applies where the processing is *necessary* for the performance of a task carried out in the public interest. As a result, personal data can be processed without consent where the processing is necessary for research carried out in the public interest, which would cover the majority of the University's research.

- **Consent** – the consent of the individual to whom the information relates provides a lawful basis for the processing of personal data, whether that consent is obtained directly from the individual concerned or indirectly by a third party contributor to the research project. However, the GDPR sets a very high standard for valid consent, as detailed at Annex A , and it may therefore be difficult to rely on consent as your basis for processing, particularly where you are relying on consent obtained by a third party on your behalf. Care needs to be taken over the form of any document seeking consent to ensure that consent has been freely given and that it includes the purposes for which the research team wish to use it. The GDPR recognises that it may not be possible to specify all the purposes of the research in advance. Researchers will therefore be expected to allow individuals to give consent only to certain areas of research or to certain parts of the project. Care should also be taken, where necessary, to document in contracts with third party contributors, the consent obligations which they are required to satisfy.

  The GDPR grants individuals a specific right to withdraw consent at any time, and it must be as easy to withdraw consent as to give it. If a research participant were to exercise this right, the research team would be obliged to stop processing that individual's data, since it would no longer have a lawful basis for processing.

- **Legitimate interests** - this applies where the processing is necessary for the University's legitimate interests or those of a third party, and those interests are not outweighed by the interests and rights of the data subjects. As a public authority, the University cannot rely on legitimate interests for any processing it does to perform its public interest tasks. However, legitimate interests may be the appropriate legal basis where it would be difficult to demonstrate that the research was necessary to meet a public interest, for example, because the research was funded by a private company and was commercial in nature. The ICO recommends that those considering this basis should undertake a Legitimate Interests Assessment (LIA), comprising three parts. The first part involves identifying the legitimate interests in question; the second

determining whether the processing of personal data is necessary to meet those interests; and the third determining whether those interests are outweighed by the rights and interests of the research participants.

Special category data

To process *special category personal data*, in addition to identifying a lawful basis for processing, as described above, researchers must satisfy one of a further set of conditions. The conditions most relevant to research projects are:

a) **Explicit consent** – consent to use special category personal data requires the research team to obtain that consent explicitly. This means that the consent must be provided in the form of an express statement to that effect ('I consent to my data being processed for….'). As above, data subjects must have the right to withdraw their consent at any time;

b) **Self-publication** – this applies where an individual deliberately makes special category personal data about themselves public. By making the information public, the individual has effectively waived their privacy interests in the information, but researchers still need to abide by the duty of fairness as described above;

c) **Medical purposes** – in this context *medical purposes* means the purposes of preventative or occupational medicine, the assessment of the working capacity of an employee, medical diagnosis, the provision of health care and treatment, and the management of healthcare services. The condition applies where the processing is pursuant to a contract with a health professional. Researchers should note that *health professional* is defined narrowly; or

d) Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes – this will apply so long as technical and organisational measures are in place to provide appropriate safeguards for the rights of research participants, as described on pages 11 and 12 below, and provided the research is in the public interest. This public interest requirement is separate and beyond that relating to the lawful basis for processing described on page six i.e. the fact that public interest task is the lawful basis for processing is not sufficient to demonstrate that the processing of special category data is in the public interest.

Researchers should note that each of the conditions described above is in addition to any conditions which might be set by the applicable body for ethical review and approval. Ethics committees are generally alive to issues of data protection and in many cases their conditions will overlap with those discussed above, but ethics committees do not provide legal advice and cannot waive any obligation arising under the GDPR. Even so, the consideration given to data protection as part of the ethical review process will help to demonstrate the University's compliance with the GDPR, and in particular the need to embed data protection requirements into processing activities ('privacy by design').

Lawful - selecting a lawful basis for the processing of personal data and/or an additional condition for the processing of special category data

In view of the potential difficulties that researchers may have satisfying the higher standard of consent required under the GDPR, and the need to respect its withdrawal, the **University recommends** that researchers should not seek to rely on consent as their legal basis for the processing of personal data. For the same reason, it is recommended that researchers should not select explicit consent as their additional condition for legitimating the processing of special category data. Rather, it is recommended that researchers should rely on public interest task as the legal basis for the processing of personal data; and research (paragraph d) above) as the additional condition for the processing of special category data.

There will continue to be a need to seek consent from participants in research in order to satisfy ethical considerations, but this will be separate from, and in addition to, the requirement under

the GDPR to identify a lawful basis for the processing of personal data and to meet a condition for the processing of special category data. How the consent is sought in such cases will depend on the nature of the project. For small-scale projects that do not involve data of a sensitive nature, it may be sufficient to use an opt-out approach to obtain consent from participants, provided they have been given adequate information about the use of their data, in accordance with the enhanced transparency requirements outlined below. The rationale and justification for using an opt-out approach to recruitment and consent should always form part of any application for ethical review. For larger projects and/or for those involving special category data, it would be more appropriate to seek positive, opt-in consent, even where consent is not the legal basis for processing. However, in either case, the wording of such consent should be careful not to conflate the issues of consent to participate in the project and "consent" to the University's use of personal data under the GDPR.

Transparent processing

Data obtained direct from the participants

When you are collecting personal data from the individuals concerned (or, in the case of research involving children, from their parents or guardians), you need to be clear, open and transparent with those individuals, by setting out what you intend to do with their data. Specifically, the GDPR requires that you provide them with the following information (this is known as the **prescribed information**):

- the name of the data controller(s) (i.e. the University and any co- or joint data controllers if relevant) and the contact details of the data protection officer;
- the purposes for which the data are intended to be processed,
- the legal basis for processing;
- the intended recipients or categories of recipients with whom the data are to be, or may be, shared;
- if applicable, the fact that the data shall be transferred outside of the European Economic Area (the "**EEA**") and the safeguards that will apply to that transfer;
- the period for which the data will be stored, or, if that is not possible, the criteria that will be used to determine the retention period ;
- if processing is based on consent, the data subjects' right to withdraw consent at any time; and
- the data subjects' rights under the GDPR (right to access their data, right to request rectification or erasure of their data, right to object to processing, right to lodge a complaint with the ICO).

For research this prescribed information is often provided to data subjects in the form of a privacy notice or participant information.

Researchers should consider how they will ensure that *all* participants (or parents/guardians of child participants) are provided with the correct prescribed information. Whether the prescribed information is provided in a written format, read out to them or otherwise made available to them will depend on the nature of the project and the usefulness of that format to the participants. Above all, the prescribed information should be provided in a user-friendly way that avoids unnecessary jargon, and you should always document that you have provided this, particularly if the prescribed information is read out to data subjects.

Data obtained from a third party

Many research projects across the University, however, do not collect personal data directly from the individual participants, but instead involve contributions of data from other research projects or other third parties. In these cases, you are still required to provide the individual participants with the prescribed information, as detailed above, together with the following additional information:

- the categories of personal data to be processed; and
- the source of the personal data, and, whether it came from public sources.

However, you do not need to provide the prescribed information if the participants already have the information; or if doing so would involve a disproportionate effort; or prevent or seriously impair the achievement of the research objectives. Even so, you must still make the prescribed information publicly available.

2. Collected for specified, explicit and legitimate purposes

This data protection principle is clearly consistent with the requirement to provide individuals with certain prescribed information. It follows that where you have obtained personal data for a specified purpose, you should not then be allowed to use it for other purposes (i.e. 'further processing') that are incompatible with that original purpose. However, the GDPR states that the further processing of data for research purposes will be considered compatible with the original purpose for which the data was collected. There is therefore a general presumption that data collected for a non-research purpose may be reused for research purposes. However, it will still be necessary to provide the prescribed information to the data subjects, and to do so before the further processing takes place. It would also be necessary to seek consent for the new purpose, if it was the intention to rely on consent as the lawful basis for processing.

3. Adequate, relevant and limited to what is necessary for the purposes concerned (data minimisation)

This data protection principle is intended to prevent the collection of unnecessary personal data. Given the sensitivities associated with personal data, it follows that no organisation should hold personal data which it does not require. However, this data protection principle also imposes an obligation to ensure that such data is suitable for the researchers' purposes.

The GDPR emphasises that the principle of minimisation applies to all aspects of processing, and not just the amount of data collected. It is therefore important for researchers to consider their obligations under this principle in relation to each aspect of work that involves the processing of personal data. For example, it may not be necessary for every member of the research team or for collaborators to have access to the full data set and it may be possible to provide information to those persons in an anonymised or pseudonymised form. Access to personal data should always be restricted to those people with a legitimate need to know. Researchers should also consider whether they need to use personal data at all or whether they would be able to meet their objectives with anonymised, aggregated or pseudonymised data. See also pages 11 and 12 below.

4. Accurate and, where necessary, kept up-to-date

This data protection principle relates to the above principle: where data is not kept up-to-date it may cease to be adequate and relevant for the purposes for which it is to be processed. Accordingly, its retention will cease to be necessary for the purposes for which it was collected.

Every reasonable step should be taken to ensure that data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay. However, many research projects intend to create static archives, where updating would defeat the purpose. In these cases, it follows that researchers do not need to keep the personal data up-to-date.

5. Not be kept as identifiable data for longer than necessary for the purposes concerned

This data protection principle also relates to the third principle above: retaining personal data in an identifiable form for longer than necessary means the data will no longer be relevant. The GDPR does not specify how long personal data should be held for, although a specific retention period may be required under other legislation or as a result of regulatory or policy considerations. In all cases the retention period, or at least its basis and rationale (if not the precise detail), will need to be communicated to the research participants in order to satisfy the requirement for transparency under the first data protection principle (pages 8 and 9 above).

6. Processed securely

Information security breaches may cause serious harm or distress to individuals or less serious embarrassment or inconvenience, but individuals are entitled to be protected from *all* forms of security breach.

The GDPR requires researchers to take appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. It should be noted that the requirements of the GDPR go beyond the way information is stored and transmitted, relating to every aspect of the processing of personal data. Security measures should seek to ensure that: (a) only authorised people can access, alter, disclose or destroy personal data; (b) those people only act within the scope of their authority; and (c) if personal data is accidentally lost or destroyed it can be recovered to prevent any damage or distress to the individuals concerned.

There is no panacea for information security, but researchers should periodically consider technological advancements in security and the costs of implementing those technologies and liaise with the IT and/or Information Security teams as appropriate. It is also important to ensure that all staff and students involved in research using personal data receive training in data protection and information security. The level of security that a research project adopts will depend on the risks associated with that project. In particular, the GDPR says that those measures should be *appropriate* to (a) the nature of the information in question and (b) the harm that might result from its improper use, or from its accidental loss or destruction e.g. e.g. identity fraud, distress at the exposure of private or sensitive information.

The physical security of personal data includes factors such as the quality of doors and locks and whether the premises are protected by alarms, security lighting or CCTV; but it also includes how access to the premises is controlled, the supervision of visitors, the disposal of paper waste and the security of portable equipment (e.g. laptops and any storage media or devices). Computer security is constantly evolving and may require specialist advice.

Other requirements

Accountability

The GDPR introduces a new requirement for accountability; data controllers must be able to demonstrate that they are complying with the data protection principles and other requirements of the GDPR. It is essential therefore that researchers document any policies or procedures they adopt in order to comply with data protection requirements. Similarly, if they rely on consent as their legal basis for processing, they must be able to demonstrate that the individual has consented by maintaining a record of when consent was obtained, how it was given and what the individual was told at the time.

As part of this emphasis on accountability, data controllers are also required to keep records of their processing activities, which will be subject to inspection by the ICO, particularly in the event of any security breach. These records must show the categories of data subject (from whom they collect the data), the categories of personal data (what types of data they collect), the categories of recipient (what other parties the data is shared with, if applicable), details of any transfers of personal data to a third country (i.e. outside the EU), the time limits for erasure, and a general description of security measures. Whilst it is expected that researchers will already keep detailed records as part of their normal data management responsibilities, they need to ensure that these are sufficient to satisfy the GDPR's record-keeping requirements.

Appropriate safeguards

The GDPR requires that organisations processing personal data for research purposes adopt technical and organisational measures to provide appropriate safeguards for the rights and freedoms of the data subject, and that those safeguards should in particular ensure respect for the principle of data minimisation. Pseudonymisation, where it would not undermine the function of the research, is mentioned as one example of an appropriate safeguard but in general the GDPR is not prescriptive as to what form the safeguards should take. However, the GDPR expects researchers to use anonymised or pseudonymised data if such data is sufficient for their purposes. It is particularly important therefore that researchers are able to demonstrate that they have given proper consideration to the question of whether they could achieve their objectives without the use of fully identifiable personal data.

The Data Protection Bill supplements the GDPR by stipulating that the requirement for appropriate safeguards will not be met if the processing is likely to cause substantial damage or substantial distress to a data subject or if it forms the basis for decisions or measures relating to a particular individual. (The latter condition will not apply to interventional medical research that has been approved by a NHS Ethics Committee.)

Data sharing agreements

At present, the ICO recommends as good practice that organisations that share personal data for specific purposes should have a written agreement in place setting out their respective roles and responsibilities. Under the GDPR, it will be compulsory for joint data controllers (i.e. organisations that jointly decide how and why personal data should be used) to have such an agreement in place, and for this to indicate in particular their respective responsibilities in relation to data subjects, including which controller will be responsible for providing the prescribed information. This requirement will affect any research project carried out in collaboration with other institutions where the purposes and means of processing are decided jointly. Researchers should seek advice from Research Services with respect to all such agreements.

Data processors

If a researcher is using a third party to collect or process personal data on its behalf (a 'data processor'), it must have a written agreement with that third party. The GDPR is quite prescriptive in terms of what such a written agreement must say. Researchers should seek advice from Research Services with respect to all such agreements.

Data Protection Impact Assessments

At present, the ICO recommends that, as a matter of good practice, organisations carry out a Privacy Impact Assessment when planning a new project that involves the processing of personal data. Under the GDPR, it will be compulsory to carry out a Data Protection Impact Assessment ("**DPIA**") (the new term for a Privacy Impact Assessment) for any project that is likely to pose a 'high risk' to the rights and freedoms of individuals. (Such an assessment is part of the general requirement for 'privacy by design/default', whereby data protection requirements are to be embedded into systems and processes from the beginning.) The GDPR

does not define 'high-risk' but gives as one example the 'large-scale' processing of special category data. It is likely therefore that a DPIA will be required for some research projects, particularly those in the medical field. The ICO is required to publish a list of the types of processing operations requiring a DPIA and further guidance will be issued once this list is available. Even if a full blown DPIA is not necessary, researchers need to be in a position to demonstrate that they have proactively addressed the data protection implications of their projects, in order to comply with the requirements for accountability and privacy by design.

G. Can personal data be transferred to a country or territory outside the EEA?

There is a general prohibition on transfers of personal data outside of the EEA unless these transfers are subject to quite narrowly prescribed conditions and safeguards.

The University clearly works with many organisations in countries and territories which fall outside of this region, but this does *not* mean that the University cannot supply, or provide access to, personal data to organisations in those countries. It does, however, mean that researchers need to comply with the conditions for transferring personal data to such countries and territories.

Please note that if you move to another institution which is located outside the EEA, and the University has permitted you to take research data with you, this will count as a transfer of data.

Transfers of personal data to a country or territory outside the EEA may take place if one of the following conditions are complied with:

- **Transfer on the basis of an adequacy decision.** The European Commission considers the data protection laws in that country or territory ensures an adequate level of protection for data subjects. To date, only the following have passed the test: Andorra, Argentina, Canada (for commercial organisations), Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand and Uruguay. In addition, a transfer to a US company that has been certified under the EU US Privacy Shield Framework will be regarded as legal under the GDPR. The list of companies that are certified under the Privacy Shield can be searched here.

- **Transfer subject to appropriate safeguards.** Transfers may occur if the controller and processor have provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. This includes (most commonly) the use of standard contractual clauses which have been approved by the European Commission.

Researchers should seek advice from Research Services for advice on all research-related agreements, including when seeking to legitimise transfers of personal data outside the EEA under standard contractual clauses, Privacy Shield or otherwise.

Cloud service providers

Researchers need to bear in mind that using international cloud-based services e.g. Dropbox, may involve a transfer of personal data outside the EEA. Even if the service in question has signed up to the EU-US Privacy Shield (see above), it may not be appropriate to use such a service, since the terms and conditions tend to be one-sided, and are unlikely to be sufficient to enable the University to meet all its obligations under the GDPR. If you sign up to a cloud service in your role as a member of staff, you may be binding the University, and not just yourself, to the cloud service's contractual terms. The risks will be greater where the personal data involved is confidential or sensitive. You therefore need to think carefully about whether you could use an alternative service that complies fully with the GDPR or whether you could use the service without sharing personal data.

H. Are there any relevant exemptions?

There are a number of exemptions from specific duties and obligations granted to processing that is carried out for the sole purpose of research. Some of these exemptions have been discussed above in the relevant sections to which they pertain.

Reuse of personal data for research

Whilst under the second data protection principle, the further processing of personal data is stated as only being allowed where it is compatible with the purposes for which it was originally collected, the GDPR provides a presumption that research is compatible with the purposes for which the data was obtained. Care must still be taken to ensure that any further use is compliant with all other relevant obligations under the GDPR e.g. transparency

Research as an acceptable condition for processing of special category data

The processing of special category personal data is generally prohibited, unless one of several available conditions is met. Processing which is necessary for research purposes in the public interest is one such condition rendering the processing legal.

Retention

The fifth data protection principle requires that data be kept as identifiable data for no longer than is necessary to meet the purposes for which the data is processed. However, personal data which are processed for research purposes may be kept for 'longer'. (We are awaiting guidance from the ICO as to how the term 'longer' should be interpreted.)

Transparency

If personal data processed for research has been collected from a third party and not directly from the individuals concerned, it will not be necessary to provide the prescribed information directly to each individual if doing so would require a disproportionate effort or if it would prevent or seriously impair the achievement of the research objectives. Even so, you must still make the prescribed information publicly available.

Individual rights

The GDPR grants individuals new or improved rights in relation to their personal data, including the right to access the data, the right to object to processing, the right to request that the data be deleted (the right to be 'forgotten'), the right to request that the processing of the data be restricted and the right to request the rectification of inaccurate or incomplete data. However, these rights are in any event not absolute; and where personal data is processed solely for the purposes of research, these rights will not apply to the extent that they would prevent or seriously impair the achievement of those purposes.

If researchers receive requests of the kind described above, they should refer them to the Information Compliance Team for action.

The above exemptions are only available where the processing satisfies the requirement for appropriate safeguards, as described above.

I. Practical considerations

This section is intended to highlight some of the issues that researchers may need to consider at different stages of their project. It is extremely difficult to highlight all of the issues which may arise during the course of every project and, accordingly, this section does not purport to be exhaustive.

- **Self-collection** – if researchers are collecting personal data directly from individuals, has consideration been given to the conditions for processing and the provision of the prescribed information?

- **Third-party processing**– if researchers are using a third party to collect or process personal data on their behalf (a data processor), they need to get advice from Research Services to enter into an agreement with that third party to ensure the information is processed in accordance with the University's legal obligations.

- **Third-party contribution** – if researchers are obtaining personal data from a third party, they should seek assurances about the information in accordance with the University's obligations. It is important to note that if you are relying on the consent of the individuals to process any personal data, you will need to see those consents – third-party assurances alone will not be sufficient, although the ICO may take them into account in any enforcement action.

- **Security** – Have researchers considered appropriate security measures and implemented a policy for handling personal data?

- **Sharing** – if researchers are intending to share access to personal data, then they are required by law to enter into a written agreement with those parties, setting out the conditions on which the data is made available.

It should be noted that the University has prepared a growing suite of templates which can be adapted for use by researchers collecting and sharing information about individuals.

Checklist

To assist researchers verify whether their projects comply with data protection requirements a checklist is provided at Annex B. This is also available on the CUREC website.

Further information

For further information in relation to any matter raised in this note, please contact:

Legal Services Office
lsoweb@admin.ox.ac.uk

Information Compliance Team
data.protection@admin.ox.ac.uk

Annex A

Consent requirements

If consent is to be the legal basis for processing personal data, it must be freely given, specific, informed and unambiguous. In general, consent will be appropriate only where we are able to offer the individual a genuine choice over whether and how their data is used.

The data subject should show their agreement to the processing of their personal data by a statement or a clear affirmative action, such as ticking a box or signing a form. This means that consent can be expressed only through a positive opt-in and not through a failure to opt-out.

If the request for consent is in writing it should be in an intelligible and easily accessible form, using clear and plain language.

Data subjects have the right to withdraw consent at any time, and it must be as easy to withdraw consent as it is to give it. Data subjects must be informed of their right to withdraw consent at the same time as they are asked to provide it.

The GDPR stipulates that consent will not be regarded as freely given if:

- an individual is offered a service that depends on his/her giving consent for unrelated processing activities; or
- an individual is not allowed to consent separately to different types of processing activities; or
- there is a clear imbalance in power between the organisation and the individual, particularly where, as with the University, the organisation is defined as a public authority. There is no absolute ban on public authorities relying on consent but it must be emphasised to the individual that they will not suffer any detriment if they choose to refuse consent.

Annex B

Data Protection Checklist

Section 1 should be considered when drafting information for participants and consent forms.

Sections 2 to 9 should be considered when completing the sections in the ethics application form referring to the Managing and Handling of Personal and other Research Data

Transparency
1. Does the information to be provided to participants indicate:
a. the purposes for which their personal data/special category data will be processed?
b. the people or organisations their personal data/special category data will be shared with?
c. the legal basis for the processing of their personal data/special category data? NB. For the majority of University research, it is recommended that `public interest task' is the appropriate legal basis.
d. any international transfers of their personal data/special category data?
e. when their personal data/special category data will be erased? NB. The GDPR requires that data is not kept as identifiable personal data for longer than is necessary in relation to the purposes for which it is processed. However, personal data processed solely for research purposes may be stored for longer periods, provided there are appropriate safeguards, such as pseudonymisation. This longer period is not defined in the GDPR. You will also need to comply with the University's policy which stipulates that research data and records should be retained for a minimum of three years after the end of the research, or longer if required by research funders and regulators – see http://researchdata.ox.ac.uk/funder-requirements/ .
f. their rights under the GDPR?
Data minimization
2. Are the items of personal data/special category data to be collected the minimum necessary to achieve the research objectives?
3. Has the potential for using anonymised or pseudonymised data been considered?
4. Will access to the personal data/special category data of participants be restricted to authorised persons?
5. Will participant data be kept in the form of fully identifiable data for a fixed period of time?
6. Is there a clear rationale for the length of time data will be kept as fully identifiable data? (see 1e. above)
Security
7. Will personal data/special category data be collected, transmitted and stored securely?
8. Is the level of security to be provided appropriate to the risks represented by the processing?
9. Will arrangements be put in place for the secure disposal and or destruction of personal data/special category data when it is no longer required?

Other safeguards
10. If the data is to be shared with another organisation, will there be a written agreement with the other organisation, setting out each one's respective roles and responsibilities, and how individuals may exercise their rights in respect of their data?
11. Will the personal data/special category data of participants be used for measures or decisions with respect to individual participants?[3] [If the answer to this question is 'Yes', the processing of the personal data will not comply with the Data Protection Bill/Act and the GDPR.]
12. Is it likely that your use of personal data/special category data will cause substantial damage or substantial distress to any of the participants?

[3] Questions 11 and 12 reflect the requirement in the Data Protection Act that personal data may not be used for research purposes if: (a) it is processed for the purposes of measures or decisions with respect to particular individuals; or (b) it is likely to cause substantial damage or substantial distress to an individual.