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 Data Protection Act 1998, and to assist their preparation for research projects. In particular, this note addresses the following questions and issues:

Research teams may need further guidance, particularly in applying legal requirements to specific projects. This is available from the University's Data Protection 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 research teams collecting and sharing information about individuals.

A. What is data protection?

Technology has made it possible to collect and use increasing amounts of information about individuals in ever more diverse ways. The Data Protection Act 1998 (the "**Act**") introduced a new framework to safeguard the rights of those individuals.

In policy terms, the Act 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 research teams cannot make use of such information, or even that research teams must always have an individual's consent to do so, but it does impose controls and restrictions which must be complied with.

B. Why is data protection important?

Compliance with the Act is a legal requirement. Breaches of the Act may result in investigations, significant fines, adverse publicity, and civil or criminal liability. Enforcement proceedings may be brought by the Information Commissioner's Office (the "**ICO**"), the Director of Public Prosecutions or, in certain circumstances, the individuals to whom the information relates.

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

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

The Act only applies to the "**processing**" of "**personal data**". It will usually be obvious whether your project falls within the scope of the Act, 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: obtaining 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 data?

Data means practically all forms of information that the University might hold. However, it should be noted that the Act is primarily concerned with information which is (a) held, or intended to be held, on computer; or (b) held in manual records which are sufficiently structured so as to allow ready access to specific information about individuals.

Most research projects will involve information falling within the two categories above, but where a project involves information falling outside of these categories, it may be exempt from *some* of the rights and duties arising under the Act (see section G below).

3. Is that data personal?

Personal data is information which relates to a living individual who can be identified (a) from those data; or (b) from those data and any other information which is in the possession of, or likely to come into the possession of, anyone who may have

access to it. This includes any expression of opinion about the individual and any indication of the intentions of any person in respect of the individual. The information does not have to be factually correct in order to be personal data.

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, the information will not constitute personal data and the duties and obligations of the Act will not apply.

Research teams 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 he belongs.

In determining whether an individual is identifiable, account should be taken of all the means likely reasonably 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 his identity.

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 research team (or any other team or person operating within the University) possesses the means to identify any of the individuals to whom the information relates, that information will 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 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 Act.

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.

Data relating to dead people

You will note that the definition of personal data contains a reference to "living individuals". However, research teams should be aware that a dead person's information will be indirectly protected under the Act where that information also relates to a living person. For example, information that a dead man suffered from haemophilia would indicate that his daughter carries the disease, as it is linked to a gene on the X-chromosome.

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, research teams 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 sensitive personal data?

The Act recognises that some categories of personal data are particularly private and could be used in a discriminatory way. As a result, the Act requires research teams to treat this "**sensitive personal data**" with greater care.

> *Sensitive personal data* includes any personal data consisting of the following information: race or ethnic origin; political opinions; religious or other beliefs; trade union membership; health; sexuality; or alleged or actual criminality.

Due consideration should be given to information which may indirectly disclose sensitive personal data about an individual. For example, photographs and names may give an indication of a person's race or religious beliefs. The additional legal requirements in relation to sensitive personal data are described below (see section F).

E. Who is responsible for complying with the Act?

The Act imposes obligations on the "**data controller**". This means the person who (either alone or jointly or in common 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, or are you acting pursuant to someone else's instructions?

For research projects based at the University, the University is the data controller and it is registered with the ICO for this purpose. You are required by your employment contract with the University to comply with the Act. Where the University is the data controller and you intend to supply any personal data to a third party to perform any subcontracted work, the University will be liable for their non-compliance with the Act and such transfer *must* be made under an appropriate contract.

Where the University is not the data controller in respect of any personal data (e.g. where work is subcontracted to the University), the University still requires you to treat such personal data in accordance with the data protection principles (see section F below).

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

Research teams must process all personal data in accordance with the eight "**data protection principles**", unless there is a relevant exemption (see section G below).

Data protection principles

Personal data must:

1. be processed fairly and lawfully;
2. be obtained and processed for specified purposes;
3. be adequate, relevant and not excessive for the purposes concerned;
4. be accurate and, where necessary, kept up-to-date;
5. not be kept longer than necessary for the purposes concerned;
6. be processed in accordance with the individual's rights under the Act;
7. be processed securely; and
8. not be transferred to a country or territory outside the European Economic Area.

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

1. Fair and lawful processing

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

Duty to process lawfully

It is easy to overlook the reference to *lawful* processing. Essentially, if your collection and use of any personal data is unlawful under any other statute or rule of common law, your compliance with the provisions of the Act will not legitimise or otherwise make that collection and use lawful. When research teams are operating in countries and territories outside the United Kingdom, then they should consider whether their actions are lawful in those countries and territories.

Duty to process fairly

The duty to process personal data *fairly* is also comprised of two elements. First, when you are collecting personal data from the individuals concerned, there is the duty to be clear, open and transparent with those individuals about how their personal data will be used. Indeed, you are required to provide them with certain "**prescribed information**". The prescribed information in a research context must include:

- the name of the data controller (i.e. the University);
- the purposes for which the data are intended to be processed;
- the intended recipients or categories of recipients with whom the data are to be, or may be, shared; and
- any additional information in respect of your project which is necessary to ensure that your processing is fair.

There is no requirement for this prescribed information to be provided in writing, but research teams should consider how they will ensure that *all* 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. The prescribed information is often incorporated into a participant consent form.

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. In these cases, you are still required to provide the individual participants with the prescribed information unless doing so would involve a disproportionate effort. This exemption is unlikely to apply where you have the individuals' contact details, or access to them, regardless of the number of participants involved.

Secondly, there is the general duty to process personal data fairly. This requires research teams 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 (see comments on the sixth data protection principle below).

Conditions to processing

Finally, you are required to demonstrate that you have complied with at least one of the conditions to processing personal data and, in the case of sensitive personal data, one of the further conditions required to process that information. The conditions which are most likely to apply to research projects are discussed below.

Research teams must be able to demonstrate one of the following conditions in the processing of *all* personal data:

- **Consent** – the consent of the individual to whom the information relates is the most effective means of achieving fair processing, whether that consent is obtained directly from the individual concerned or indirectly by a third party contributor to the research project. Care needs to be taken over the form of any document seeking consent to ensure that it includes the purposes for which the research team wish to use it. Care should also be taken, where necessary, to document in contracts with third party contributors, the consent obligations which they are required to satisfy; or

- **Legitimate interests** – this applies where (a) the processing is *necessary* for the purposes of legitimate interests pursued by the University, or a third party, and (b) that processing does not cause prejudice to the rights and freedoms or legitimate interests of the individual. As a result, personal data can be processed without consent where the University's legitimate interests outweigh any privacy concerns of the individual. To make responsible use of this condition, research teams must carry out a thorough evaluation exercise, balancing any competing interests. Research teams may, however, find that they still need to provide the individuals concerned with the prescribed information (see above).

Where a research project involves *sensitive personal data* the researchers must also be able to demonstrate that they have satisfied one of the following conditions:

- **Explicit consent** – whereas the condition based on consent above allows research teams to infer consent in certain contexts (e.g. where an individual responds to an open invitation to participate in the research project by supplying information), any use of sensitive personal data requires the research team to obtain that consent explicitly. This is often achieved by asking the individual to sign a consent form;

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

- **Medical purposes** – in this context *medical purposes* means the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment, and the management of healthcare services. The condition applies where (a) the processing is *necessary* for any medical purpose and (b) is undertaken by a healthcare professional or a person who, in the circumstances, owes a duty of confidentiality which is equivalent to that which would arise if the person were a healthcare professional. Research teams should note that *healthcare professional* is defined narrowly, but an equivalent duty of confidentiality can be achieved contractually; or

- **Public interest** – this applies where the processing: (a) is in the *substantial* public interest; (b) is *necessary* for research purposes; (c) does not support measures or decisions with respect to any particular individual; and (d) does not cause, nor is likely to cause, *substantial* damage or *substantial* distress to the individual concerned or any other person. Research teams should note that this condition sets the bar relatively high.

Research teams 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. These bodies are generally alive to issues of data protection and in many cases their conditions will overlap with those discussed above, but ethics bodies do not provide legal advice and cannot waive any obligation arising under the Act.

2. Obtained and processed for specified purposes

The second 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 where they are incompatible with that original purpose.

Accordingly, where a research team wishes to use personal data collected for the purposes of a different research project, it will need to consider whether the new purpose is compatible with the original purpose or whether it needs to obtain fresh consent from the individuals concerned. However, where the research exemption (see section G) applies, you may find that you do not need to obtain fresh consent, although you will still have to consider whether you need to provide the prescribed information (see above).

3. Adequate, relevant and not excessive for the purposes concerned

The third 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, the third data protection principle also imposes an obligation to ensure that such data is suitable for the research team's purposes.

It is important for research teams to consider their obligations under this principle in relation to each aspect of work to be performed by the research team. 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 anonymous or pseudonymous form. Access to personal data should always be restricted to those people who have a need to access it.

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

The fourth data protection principle relates to the third 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 be excessive.

However, many research projects intend to create static archives, where updating would defeat the purpose. In these cases, it follows that research teams do not need to keep the personal data up-to-date.

5. Not kept longer than necessary for the specified purposes

The fifth data protection principle also relates to the third principle: retaining personal data for longer than necessary amounts to the holding of excessive data. The Act does not specify how long personal data should be held for, although other legislation may give rise to an obligation to hold certain types of data for a specified period. In the absence of any legal requirement, research teams will need to consider this question in the context of their particular project. However, where the research exemption applies (see section G), you may not have to comply with this requirement.

6. Processed in accordance with the individual's rights under the Act

The sixth data protection principle relates to the following rights of individuals under the Act: (a) a right of access to personal data held about him; (b) a right to prevent processing of personal data which is likely to cause damage or distress to the individual; (c) a right to prevent the processing of personal data for the purposes of direct marketing; and (d) a right to require that no decision which significantly affects the individual is based solely on automatic processing of personal data.

For the purposes of most research projects, the only rights which are likely to be relevant are those stated at (a) and (b) above. However, where the research exemption applies (see section G below), those personal data are exempt from the right stated at (a), and the conditions for that exemption make it unlikely that the right stated at (b) will apply.

7. 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. To date, breaches of the seventh data protection principle account for the majority of fines issued by the ICO.

The Act requires research teams to take appropriate technical and organisational measures 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 Act 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 research teams should periodically consider technological advancements in security and the costs of implementing those technologies. The level of security that a research project adopts will depend on the risks associated with that project. In particular, the Act 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.

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.

It is important to understand that where a research team uses any third party to process personal data on its behalf, the University will be held responsible for any breach of the obligations under the Act by that third party. Moreover, there are a number of conditions which apply to the use of such third parties (see section H), including a written contract requiring them to comply with obligations equivalent to those imposed by the seventh data protection principle.

8. Not transferred to a country or territory outside the EEA

The generality with which the prohibition is stated should not cause panic. It is possible to transfer personal data outside the EEA, but you have to be able to demonstrate one of the conditions for doing so.

Please note that while the European Economic Area (the "**EEA**") is often confused with the European Communities and the European Union, it is actually a larger region which includes the 27 member states of the European Union and the European Free Trade Association states (Norway, Lichtenstein and Iceland).

Strictly speaking, the eighth data protection principle prohibits the transfer of personal data to a country or territory outside the EEA *unless* that country or territory ensures an adequate level of protection for the rights and freedoms of the individuals to whom those personal data belong.

You are strongly advised not to make a determination of adequacy – to do so would require a careful analysis of (a) the nature of the personal data; (b) the country or territory of origin of the personal data; (c) the country or territory of final destination of the personal data; (d) the purposes for which and the period during which the data are intended to be processed; (e) the law in force in the country or territory in question; (f) the international obligations of that country or territory; (g) any relevant codes of conduct or other rules which are enforceable in that country or territory; and (h) any security measures taken in respect of the data in that country or territory.

Since 1995, the European Commission has considered the adequacy of data protection laws in many countries and territories, but only the following have passed the test:

Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, and Jersey.

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 research teams need to comply with one of the conditions for transferring personal data to such countries and territories.

The easiest way for research teams to comply with this requirement is to use the University's standard contractual clauses for transferring data outside the EEA. This will also serve to meet the research team's obligations under the seventh data protection principle (see above).

G. Are there any relevant exemptions?

The most relevant exemptions are discussed below, but it is important to note that these are not blanket exemptions: they will only operate to exempt research teams from *specific* duties and obligations under the Act.

1. Research exemption

This exemption applies to the processing of personal data for *research purposes*, a term which includes statistical or historical purposes. The exemption applies as follows:

- the further processing of personal data *only* for research purposes is not to be regarded as incompatible with the purposes for which they were obtained, notwithstanding the second data protection principle;

- personal data which are processed *only* for research purposes may, notwithstanding the fifth data protection principle, be kept indefinitely; and

- personal data which are processed *only* for research purposes are exempt from an individual's right of access to data held about him if the results of the research are not made available in a form which identifies any participant.

In each case, research teams will need to be able to demonstrate that the personal data are not processed:

- to support measures or decisions with respect to particular individuals; and

- in such a way that *substantial* damage or *substantial* distress is, or is likely to be, caused to any individual.

2. Public authority exemption

The definition of *data* (see section C above) includes all recorded information held by a public authority (the University is a public authority) which is not processed by computer or held in searchable manual records. This category of data was introduced by the Freedom of Information Act 2000 (the "**FOIA**") and is intended to protect information relating to individuals which might otherwise be disclosable under a FOIA request.

Since this category of data was never intended to be protected by the Act, it follows that it enjoys broad exemptions. It should, however, be noted that most research data will not fall into this category and, accordingly, the exemption will not be available. If you think your research data falls into this category, please contact the Data Protection Team or the Legal Services Office for further information.

3. Other exemptions

In addition, there are exemptions in relation to: national security; crime and taxation; health, education and social work; regulatory activities; journalism, literature and art; information available to the public by or under an enactment; disclosures required by law or under legal proceedings; parliamentary privilege; domestic purposes; and more. Please contact the Data Protection Team or the Legal Services Office for more information about any of these exemptions.

H. Practical considerations

This section is intended to highlight some of the issues that research teams 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 the research team is collecting personal data directly from individuals, has consideration been given to the conditions for processing and the provision of the prescribed information?

- **Third-party collection** – if the research team is using third parties to collect personal data on its behalf, the team should be thinking about entering into an agreement with those third parties to ensure the information is collected in accordance with the University's obligations.

- **Third-party contribution** – if the research team is reliant on third parties voluntarily contributing personal data, the team 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** – has the research team considered appropriate security measures and implemented a policy for handling personal data?

- **Sharing** – if the research team is intending to share access to personal data, then it is 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 research teams collecting and sharing information about individuals.

I. The future of data protection law

The Act was designed to implement the European Data Protection Directive (95/46/EC). In 2009, the European Commission commenced a review of the legal framework for data protection within the European Union. The Commission intends to:

- modernise the EU legal system for the protection of personal data, in particular to meet the challenges resulting from globalisation and the use of new technologies;

- strengthen individuals' rights, and at the same time reduce administrative formalities to ensure a free flow of personal data within the EU and beyond; and

- improve the clarity and coherence of the EU rules for personal data protection and achieve a consistent and effective implementation and application of the fundamental right to the protection of personal data in all areas of the Union's activities.

The evidence suggests that the Commission is keen to make progress on these objectives. At the end of 2011, two draft regulations were leaked on the internet and, if genuine, it would suggest that there may be new legislation to consider within the next year or two.

Further information

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

Geoff Hemmings
Solicitor, Legal Services Office
geoff.hemmings@admin.ox.ac.uk
T 01865 (2)**70138**

Max Todd
Data Protection Team
data.protection@admin.ox.ac.uk
T 01865 (2)**80299**