**A Researcher's Guide to the Data Protection Act**

The Data Protection Act gives individuals (known as data subjects) rights regarding the personal data organisations hold about them and gives organisations responsibilities regarding that data.

Personal data is defined as data which relate to a *living* individual who can be identified from the data or from data and other information which is in the possession of, or is likely to come into the possession of, an organisation.

Sensitive personal data is further defined in the act as personal data consisting of information as to:

1. the racial or ethnic origin of the data subject
2. his political opinions
3. his religious beliefs or other beliefs of a similar nature
4. whether he is a member of a trade union
5. his physical or mental health or condition
6. his sexual life
7. the commission or alleged commission by him of any offence
8. any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

These responsibilities are codified as eight data protection principles:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
2. at least one of the conditions in Schedule 2 is met, and
3. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
4. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.**E+W+S+N.I.**
5. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.**E+W+S+N.I.**
6. Personal data shall be accurate and, where necessary, kept up to date.**E+W+S+N.I.**
7. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.**E+W+S+N.I.**
8. Personal data shall be processed in accordance with the rights of data subjects under this Act.**E+W+S+N.I.**
9. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**E+W+S+N.I.**
10. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

If you want to use personal data for your research you have two options:

* Comply with the Data Protection Act; or
* Anonymise the data that you use so that it no longer falls within the Act’s definition of personal data.

It is important to note, however, that data is only completely anonymised if it is impossible to identify the individuals from that information plus any other information that the University holds or is likely to hold. For example, if you anonymise a list of participants by giving each a number and then keep a separate list of the numbers and the names of the participants to which they refer, the data is not completely anonymised and would still qualify as personal data under the Act.

The Act makes [special provisions for research](http://www.legislation.gov.uk/ukpga/1998/29/section/33) *if* your research fulfils all of the following conditions:

* You are using the information exclusively for research purposes (includes statistical or historical research purposes). The information must have no other use, not even an incidental use.
* You are not using the information to support measures or decisions relating to any identifiable living individual (not just the data subject but anyone who may be affected by your research).
* You are not using the data in a way that will cause, or is likely to cause, substantial damage or substantial distress to any data subject.
* You will not make the results of your research, or any resulting statistics, available in a form that identifies the data subjects. For example if you use case studies in your research report you may choose to disguise the names of the individuals. However, if you describe their circumstances in detail it may be possible for someone to identify that individual, in which case you would not meet this criterion.

If you fulfil these conditions then you must comply with *all* of the requirements laid out below (in relation to the 8 principles). If you do not fulfil these conditions then you should be aware that you will have additional obligations and should contact the University’s Data Controller.

**Principle 1**

***Personal data shall be processed fairly and lawfully.***

To use personal data lawfully you must comply with all UK laws, and meet one condition from the list of conditions set out in the Act. To use sensitive personal data you must also meet one condition from the additional list of conditions.

The conditions that are most likely to apply for research using any personal data are:

* You have obtained consent from the data subject.
* You are processing personal data for the legitimate interests of the University or a third party *and* your use does not cause unwarranted prejudice to the rights and freedoms, or the legitimate interests of the data subject.

The conditions that are most likely to apply for research using sensitive personal data are:

* You have obtained “explicit consent” from the data subject. Explicit consent must be freely given, specific and informed.
* You are analysing racial /ethnic origins for equal opportunities purposes.
* Your processing of sensitive personal data “is in the substantial public interest and is necessary for research purposes and does not support measures with respect to the particular data subject except with their specific consent nor cause or be likely to cause substantial damage and distress” (The Data Protection (Processing of Sensitive Personal Data) Order 2000).

In most cases where you are using sensitive personal data you will use the explicit consent condition. For consent to be explicit individuals must have a full understanding of what you intend to do with their data and they must “opt-in”; you cannot ask them to opt-out if they object. You should keep a record that you have received explicit consent from the individual whose data you are using. The method you chose to use to collect explicit consent will depend upon the nature of your research but you may choose to:

* Ask individuals to sign a consent form (see annex A for a sample form).
* If you are asking individuals to complete a questionnaire you may decide to include a data protection statement within the questionnaire and ask individuals to sign to say they consent.

If you use a form of some sort to collect explicit consent the forms should be kept for as long as you keep the data about the individuals. Alternatively if you feel that the risk is low you may adopt a methodology which records that explicit consent has been given and then destroys the signed forms. For example if you are transferring questionnaire answers to a database you may also have a field to record that the individual gave explicit consent. However, if you later need to prove that an individual did give explicit consent this method will provide a lower level of proof, and protection under the law.

In order for your use of data to be fair you must inform data subjects of:

* What you are doing with the data
* Who will hold the data
* Who will have access to or receive copies of the data

This is known as a “fair processing notice”.

You are only relieved of the duty to provide a fair processing notice if *all* of the following conditions apply:

* The data has been obtained from a third party,
* Provision of a fair processing notice would involve disproportionate effort,
* You record the reasons for believing that “disproportionate effort” applies.

When assessing disproportionate effort you should weigh the cost, time, and ease of provision of the notice, against the benefit to the individual of receiving the notice.

**Principle 2**

***Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.***

If you have met the conditions for the research exemptions **you are exempt from this requirement**.

**Principle 3**

***Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.***

You should only keep the amount of information that you need about a person to fulfil your research. This means that you should collect all the information you need, but not more. For example if you do not need information about individuals’ dates of birth, you should not collect or hold that information.

**Principle 4**

***Personal data shall be accurate and, where necessary, kept up to date.***

This means that you must ensure that your research data is accurate. However, you will not have to keep your research data up to date unless it is necessary to do so.  For example if your research is based on information representing the situation at a particular moment in time there is no need to update the information if circumstances change.

**Principle 5**

***Personal data processed for any purpose or purposes shall not be kept for longer than is necessary.***

If you have met the conditions for the research exemptions you are exempt from this requirement.

**Principle 6**

***Personal data shall be processed in accordance with the rights of data subjects under this Act.***

The Act provides data subjects with the following rights:

* To be informed by you whether you or someone on your behalf is using his personal data.
* To be provided with a copy of his data and associated information held by you. This is known as the right to subject access.
* To block your use of his personal data if it is likely to cause unwarranted substantial damage or substantial distress to him or another.
* To require you to ensure that no decision which significantly affects him is based solely on the processing of his personal data by automatic means.
* To compensation, payable by the University, if you cause him damage, or damage and distress, by any contravention of the Act.
* In certain circumstances to require you to rectify, block, erase, or destroy his personal data.
* To ask the Information Commissioner to assess whether or not it is likely that your use of personal data has been or is being carried out in compliance with the Act.

If you have met the conditions for the research exemptions you are exempt from the requirement to provide subject access.  But you must comply with the other rights of the data subject. For example, if you receive a request from an individual asking you to stop using their information, you must take their request seriously. From an ethical perspective, researchers are encouraged to recognise the right to withdraw of participants.

**Principle 7**

***Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.***

Any personal data that you collect must be kept securely. You must arrange your working environment to take account of this and you must ensure that any computers or other systems you use are secure.  The security measures you take should be proportionate to the data you are keeping. For example the security measures you take to protect sensitive personal data will be much more stringent than those used to protect personal information that is in the public domain.

There are implications if you work at home because you must ensure the same security for the personal data at home as it would receive in the office. If you do want to work at home you may choose, where possible, to anonymise the data so that it no longer falls within the Act’s definition of personal data. Alternatively you will need to make security provisions for your home office: for example, to ensure that family members or visitors are unable to gain access to the data you may decide to password protect your computer and keep your files in locked filing cabinets.

You must also make sure that when you dispose of the data that it is done securely. For example it is not enough simply to delete the files from a computer as they can still be accessed. You must either remove and destroy the computer’s hard disk or ensure that the data is overwritten.

**Principle 8**

***Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.***

Research often involves international collaboration, however the 8th data principle bans transfers of personal data outside the European Economic Area. However, you may transfer personal data to other countries if one of the following applies:

* The country you are transferring the data to has been designated as providing adequate protection for personal data. At present these countries are: Hungary, Switzerland and Argentina. Certain types of personal data may be transferred to organisations subject to the Personal Information Protection and Electronic Documents Act (or PIPED Act) in Canada. Personal data may also be transferred to the USA if the “Safe Harbor” arrangements apply. (Please contact the Data Controller for further information about transferring personal data to Canada and the USA.)
* You have obtained explicit consent from the data subject(s). This could be done by adding a question on the consent form.
* You have a contract with the recipient of the data, which puts the necessary safeguards in place. Please contact the records management section for more information about what constitutes an appropriate contract.
* You have completely anonymised the data.

**Annex A**

**Consent Form for use of personal data in research**

|  |  |
| --- | --- |
| Researcher: |  |
| Supervisor (if applicable): |  |
| Project title: |  |
| Researcher contact details: |  |
| Project details: | You may append an information sheet |
| Any other details: |  |

|  |  |
| --- | --- |
| Name of data subject: |  |
| Contact details for data subject: |  |

**To be completed by the data subject:**

I consent to my personal data, as outlined below, being used for the research project detailed above.

Description of personal data to be used for research:

|  |  |
| --- | --- |
| Signature: |  |
| Date: |  |