Data Protection and Research

1 Purpose

This document draws members' attention to the provisions of the General Data Protection Regulation 2016 and the Data Protection Act 2018 (together “the Legislation”) which relate to research activities, and outlines actions required to achieve compliance with the Legislation.

2 Background

The General Data Protection Regulation (“GDPR”) became law in May 2016. However, the GDPR allowed for a transitional period to enable organisations to achieve compliance with its provisions. This transitional period ended on 25 May 2018, at which time the GDPR came fully into force. The Data Protection Act 2018 was also passed in May 2018 in order to supplement the GDPR.

The GDPR supersedes the Data Protection Act 1998, and represents a significant extension of the scope of data protection compared to the 1998 Act. By way of examples, it provides enhanced rights for individuals, increased penalties for non-compliance, stricter requirements for consent and a strong emphasis on accountability and record keeping.

The GDPR is EU legislation which has direct effect in the United Kingdom. However, it is supported by the Data Protection Act 2018 which received royal assent on 23 May 2018.

The Legislation lays down principles of good information handling which are designed to make sure that personal data is used in a way which is fair to individuals and protects their rights.

Breaches of the Legislation may constitute a criminal offence, and may result in enforcement action being brought against Coventry University Group. It is therefore important that you follow these guidelines to ensure that you are acting in compliance with the Legislation.

3 Personal data

The Legislation applies to personal data, which are defined as any data relating to an identified or identifiable natural person. It does not apply to generic information about companies, nor to aggregated statistical data or anonymised data, nor to information about deceased individuals.

The Legislation places certain types of data under the heading ‘special category’ data. The following types of information fall into the category of special category personal data:

- ethnic or racial origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- the processing of genetic or biometric data for use in identifying an individual;
- physical or mental health data;
- information relating to an individual’s sex life or sexual orientation.

Inappropriate use of information of this kind is potentially very prejudicial to the data subject; the Legislation therefore requires that extra precautions be taken when processing sensitive personal data. Special rules also apply to the processing of personal data relating to criminal convictions and offences.

Researchers may seek to anonymise data used in research, by removing names and other personal identifiers, or by assigning a code to research subjects. However, it should be borne in mind that such actions may not be sufficient to anonymise data. For example, if a researcher retains a list of which codes have been allocated to which research subjects, the data would not be considered to be

anonymised in terms of the Legislation, as it would still be possible to identify individuals. Similarly, even if the names of research subjects are removed, it may still be possible to identify individuals by using a combination of other personal identifiers, such as age or gender. It should not be assumed, therefore, that taking steps to anonymise personal data means that the provisions of the Legislation do not apply.

4 Fair processing

The Legislation sets out the core principles for the processing of personal data. These core principles include a requirement that personal information is processed lawfully, fairly, and in a transparent manner. This requires transparency and data subjects must be informed of the purposes for which their data will be processed, the legal basis on which you are processing their information, who you are going to share their information with and the various rights which are afforded to them in relation to their information by the Legislation. You are also required to tell them if you will provide their information to any third party and if so whom as well as if you intend to transfer their information to a third country or international organisation. This fair processing statement should be provided to data subjects at the time information is initially collected about them.

If information is being obtained directly from the data subject by, for example, requesting them to complete a questionnaire, provision of the fair processing statement can be easily incorporated into this process. However, in some cases researchers will be using data obtained from a third party, rather than directly from the data subject. The fact that data was obtained from a third party does not automatically exempt the researcher from providing a fair processing statement; however, it may be possible to claim that providing such a statement would involve disproportionate effort on the part of the researcher or where they have already been provided with this information.

In deciding whether or not the disproportionate effort argument would apply, researchers should evaluate the time, cost, and ease or difficulty of providing research subjects with a fair processing statement, and balance this against the benefit/prejudice to the research subject of being provided with/not being provided with such a statement. Factors to be considered in making this evaluation include the size of the research sample, whether contact details for the individuals are already available and if not, how difficult it would be to obtain them, and the purpose and likely outcomes of the research and their effect on the individuals concerned. It is highly recommended that this evaluation process be documented in writing and if you are in doubt reference is made to the Information Governance Unit. It may be that a researcher regularly obtains personal data from a particular third party. In this case, the simplest course of action is for the researcher's fair processing statement to be provided to the data subjects at the same time as the third party provides its own statement.

5 Legitimate basis for processing

The core principles of the Legislation also require data controllers to have a lawful basis for their processing of personal data. The Legislation lists a number of lawful bases, one of which must apply before processing can take place.

Consent should not in any circumstances be relied upon automatically as the most appropriate grounds for the processing of personal data whether for research purposes or otherwise. There are a number of other lawful grounds for processing which may be more appropriate in the circumstances such as processing for the performance of a task carried out in the public interest and processing necessary for the purposes of the legitimate interests of the Coventry University Group.

Having said this, where data is being obtained directly from the data subject, the simplest lawful basis to use may be consent of the data subject to the processing. The consent should be freely given, specific, informed and unambiguous indication of the individual’s wishes. The consent should be separate to any other terms and will need to be referenced in the fair processing notice.

Where data has been obtained from a third party, and evaluation suggests that disproportionate effort would be involved in providing a fair processing statement, there will be no opportunity to obtain consent from the data subject. In this case, another legitimate basis can be used such as processing that is necessary for the pursuit of legitimate interests by the data controller, except where this would cause prejudice to the rights, freedoms or legitimate interests of the data subject or processing which is necessary for the performance of a task carried out in the public interest.

When special category personal data (see above), is being processed, the requirements for a legitimate basis for processing are even more stringent. The data controller, as well as fulfilling one of the lawful bases described above, must also fulfil one of the additional legitimate bases for processing sensitive personal data listed in the Legislation.

When special category personal data is obtained directly from the data subject, the easiest additional lawful basis to fulfil is that the data subject has given **explicit** consent to the processing. This requires a clear positive action on behalf of the data subject to confirm their consent which must be specific and unambiguous. When seeking explicit consent for the processing of special category data you should ensure that the particular purposes for which the special category personal data will be used should be stated very clearly and specifically in the fair processing statement. Again, the request for consent should be set out separately and not incorporated in any other terms. In addition whenever consent is relied upon the individual must be given the opportunity to withdraw that consent and that withdrawal needs to be made as easy as it was to give consent.

When consent cannot be obtained from the data subject, the additional lawful basis that would apply for processing special category personal data include: the processing is in the substantial public interest, processing is necessary for reasons of substantial public interest, or is necessary for scientific or historical research purposes.

6 Security

One of the core principles of the Legislation is that the personal data must be processed in a manner which ensures appropriate security for the individual's personal data so as to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage Researchers should ensure that:

- they comply with all Coventry University Group IT security policies and guidelines
- for personal data held on computer, appropriate access control mechanisms such as password protection and restricted access are applied;
- personal data held in manual files are handled in a way that prevents accidental or deliberate access by third parties e.g. by keeping data in locked filing cabinets or secure rooms;
- personal data used for research is disposed of in an appropriate way when the research has been completed. Paper files containing personal data should be shredded, and any information stored on the hard disk of a computer should be wiped by degaussing, rather than by simply deleting files;
- where personal data is processed off-site, for example when laptops are used by staff at home or when travelling, particular care is taken to prevent loss or accidental disclosures.

Further information on security issues can be found in the University's Information Security Policy and its associated guidelines.

7 Other Core Principles

The core principles of the Legislation also provide that personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. For example, if personal identifiers such as names and addresses are not required in order to carry out the research, the data subject should not be asked for this information.

8 Transfers of Personal Data outside the European Economic Area

The Legislation provides that personal data must not be transferred outside the European Economic Area (the EU countries plus Norway, Iceland and Liechtenstein) without appropriate safeguards. In most cases, this will mean that the data subject has consented to the transfer, having been made aware that consent means that their information will be available in countries with which do not have in place appropriate safeguards. This needs to be taken into account by researchers involved in collaborative projects including participants outside the EEA.

Where any personal data is to be transferred outside the EEA and you do not have consent, then you should consult the Information Protection Unit for further guidance to make sure that the appropriate safeguards are in place to ensure the security of the data which you are processing.

9 Exemptions

Fortunately for researchers, the GDPR provides exemptions from some of the data protection measures for processing of personal data for research purposes.

Article 5 (1) (a) provides that states that personal data shall be collected only for specified, explicit and legitimate purposes and shall not be processed in a manner which is incompatible with those purposes. However, in recognition of the fact that much research relies on data which was originally collected for an entirely different purpose, the GDPR provides that further processing for scientific, or historical research purposes in accordance with Article 89 (1) shall not be considered incompatible with the initial purpose.

Article 89 (1) of the GDPR provides that when processing for scientific or historical research purposes you must have in place appropriate safeguards to protect the rights and freedoms of the individual including measures to ensure that the minimum amount of data is collected and processed which may include the use of pseudonyms or anonymisation.

The GDPR includes a number of rights for individuals in relation to the processing of their personal data. Article 89 (2) allows members states to pass a law which limits the rights of the individual in relation to data processed for scientific or historical research purposes so for example to remove the individual's right to access to that data, to have it rectified, the right to restrict the processing of their data and their right to object to the processing.

Schedule 2, Part 6 of the Act sets out the derogations from the GDPR which England and Wales have adopted in relation to the processing of research data and provides that the provisions of the GDPR which govern individual's rights of access, rectification, restriction of processing and objections to processing do not apply to research data.

10 Research students

Staff who are supervising research students should be aware that the right of access (referred to in paragraph 9 above) means that research, and indeed undergraduate, students are able to see any files supervisors may hold on them. This includes assessments, references and examiners comments. Similarly, staff are entitled to see any reports, comments or complaints about them produced by the students they are supervising.

11 Ethical Approval

This document covers data protection issues only; staff carrying out research using personal data should be aware that there may be wider ethical issues and should follow the guidance provided on the Coventry University Ethics website by visiting https://ethics.coventry.ac.uk/

12 Further Guidance

The Information Governance Unit have dedicated information available to help researchers to include templates such as participant forms, consent forms, guides and checklists. To access this please visit the IGU team site on the staff portal.

You can contact the Information Governance Unit by emailing enquiry.igu@coventry.ac.uk if you have any queries in relation to data protection issues.