GDPR and Data Protection Act 2018: Implications for Research

SUMMARY

1) Data protection legislation ONLY applies to information which can be used to identify a living person – it does not apply to anonymised data or to people who have died.
2) Data Protection requirements apply to all living people wherever they live NOT just to people in the UK or EU.
3) You must be able to prove that you obtained informed consent to use personal data, i.e. please make sure that you keep electronic or paper copies of the signed consent forms.
4) Consent must be informed and unambiguous.
5) You must only use personal data in a fair way, i.e. not in a way which causes harm, is unexpected or misleading.
6) Only children aged 13 and over can provide informed consent. With younger children, the informed consent of their parent or guardian is needed to process their personal data.
7) You must tell research participants that they have the right to object to the processing of their personal data and also the right to request that their personal data is erased. You must provide contact details which enable research participants to exercise these rights.
8) You can now keep and archive personal data indefinitely (i.e. no time limit) for statistical, scientific or historical research purposes.
9) You can reuse personal data for a new purpose/study if this is compatible with the original purpose (and there is informed consent for the original purpose).
10) You MUST report any data breaches to the University immediately you discover them. The potential legal penalties for not doing so are horrific.

Introduction

This document only deals with the implications of the new Data Protection regulations for research. There are many additional implications for teaching and administration which are not covered in this document.

The EU General Data Protection Regulation became law on the 25th May 2018 and the Data Protection Act received royal ascent on 23rd May 2018 – it repeals and replaces the 1998 Data Protection Act and implements the provisions of the GDPR into UK law.

Personal Data

The definition of personal data has been broadened to include both e-mail addresses and machine-generated data generated through device use, such as location, cookies, and IP addresses, among others. It applies only to living people and only to personal data. Thus, once data has been anonymised, the GDPR no longer applies. However, anonymisation needs to be complete (not pseudonymisation).

The GDPR applies to researchers in the EU who collect personal data about a person from any country, anywhere in the world, i.e. if you are a UK based researcher collecting and processing personal information in Asia (or anywhere else), the GDPR still applies, as privacy and data protection are a human right.

You must be able to demonstrate that your research is ethically compliant; including maintaining evidence on how and when consent to collect and use information was obtained and you have to provide opportunities for individuals to view and correct information stored about them, or to withdraw consent for its use at any stage of the research.

Consent
Consent needs to be freely given, informed, unambiguous, specific and by a clear affirmative action that signifies agreement to the processing of personal data, i.e. consent MUST be opt-in and not opt-out. Consent needs to be documented (Article 7(1)), which means (in the context of research) it will be important for researchers to maintain documented and accurate records of the consent obtained from their participants.

To obtain informed consent in practice, researchers should:

- Inform participants about the purpose of the research;
- Discuss what will happen to their data (including the future archiving, sharing and use of their data);
- Indicate the steps that will be taken to safeguard their anonymity and confidentiality;
- Outline their right to withdraw from the research and how to do this.

However, for research, you do not need to fully identify the end purpose of the data analyses when the data are collected. Participants should be asked to give informed consent about the type of research their data will be used for.

Fairness

- You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
- You must be clear, open and honest with people from the start about how you will use their personal data.

Children
The GDPR contains provisions intended to enhance the protection of children's personal data and to ensure that children are addressed in plain clear language that they can understand. Only children aged 13 and over can provide informed consent. For younger children, the consent of their parent or guardian is needed.

Transparency is also key. You can raise children's (and their parents') awareness of data protection risks, consequences, safeguards and rights by:

- telling them what you are doing with their personal data;
- being open about the risks and safeguards involved; and
- letting them know what to do if they are unhappy.

This will also help them make informed decisions about what personal data they wish to share.

Transfer of Personal Data outside the EU
This is lawful to countries which the EU deems have adequate safeguards but it is also now lawful where there is informed consent to do so.

The Right to Object

- The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.
- Where the right to object applies, you may be able to continue processing if you can show that you have a compelling reason for doing so.
- You must tell individuals about their right to object.
- An individual can make an objection verbally or in writing.
- You have one calendar month to respond to an objection.

However, for scientific or historical research or statistical purposes, the right to object is limited, i.e. you do not need to erase the data if the *processing is necessary for the performance of a task carried out for reasons of public interest*.

Right of erasure

- The GDPR introduces a right for individuals to have personal data erased.
- The right to erasure is also known as 'the right to be forgotten'.
- Individuals can make a request for erasure verbally or in writing.
- You have one month to respond to a request.
- The right is not absolute and only applies in certain circumstances.

Specifically, the right does not apply for archiving purposes in the public interest or scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing.

However, the GDPR explicitly provides children with the right to change their minds about their consent, etc. and ask for their data to be erased.

Research Data Storage and re-use for research

The new 2018 DPA clears up the ambiguity in the old legislation with regard to research data storage and re-use. The new act explicitly states that:

"Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes"

This means that personal data should be anonymised as soon as practical (when anonymisation is needed) and can be archived and reused for scientific research as long as the reuse is compatible with the original purpose for which these data were collected. For example, you can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent or you have another clear basis in law for processing the data.

You can now keep personal data indefinitely if you are holding it only for:

- archiving purposes in the public interest;
- scientific or historical research purposes; or
- statistical purposes.
  (see http://www.bristol.ac.uk/staff/researchers/data/)

Although the general rule is that you cannot hold personal data indefinitely 'just in case' it might be useful in future, there is an inbuilt exception if you are keeping it for these archiving, research or statistical purposes. See advice and model consent forms at https://www.ukdataservice.ac.uk/manage-data/legal-ethical/consent-data-sharing/consent-forms

You must have appropriate safeguards in place to protect individuals. For example, pseudonymisation may be appropriate in some cases.

Data Breaches

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (Information Commissioner's Office https://ico.org.uk/). You must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

The Cyber Security Breaches Survey 2018 showed that:
"Over four in ten businesses (43%) and two in ten charities (19%) have experienced cyber security breaches or attacks in the last 12 months. This rises to seven in ten (72%) among large businesses, and a similar proportion (73%) among the largest charities with incomes of £5 million or more."

See https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018

If you lose personal data or a data breach occurs, you **MUST** notify the University immediately. This means sending an e-mail to data-protection@bristol.ac.uk and telling your Head of School. See additional details at http://www.bristol.ac.uk/secretary/data-protection/data-breaches-and-incidents/

Potential Penalties – DPA 2018

The maximum penalty is €20,000,000 – so please try not to mess up!

(Section 157) Maximum amount of penalty

The "higher maximum amount" is—
(a) in the case of an undertaking, 20 million Euros or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher, or
(b) in any other case, 20 million Euros.

The "standard maximum amount" is—
(a) in the case of an undertaking, 10 million Euros or 2% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher, or
(b) in any other case, 10 million Euros.

The maximum amount of a penalty in sterling must be determined by applying the spot rate of exchange set by the Bank of England on the day on which the penalty notice is given.