What is the GDPR?

The General Data Protection Regulation (GDPR) will replace the current UK Data Protection Act and is designed to strengthen privacy rules and requirements around how information relating to individuals can be used, updating and unifying data protection law across the Europe. It establishes new rules governing how personal data is handled by organisations, and extends the rights of individuals regarding their own personal data.
When does it become law?
GDPR comes into force in all EU nations, including the UK, on 25th May 2018.

What about Brexit?
GDPR is an EU Regulation. The UK will still be a member of the EU when GDPR comes into force in May 2018 so it will automatically apply here. When the UK leaves the EU there will need to be an equivalent standard of data protection in place if UK-based organisations can continue to process the personal data of EU citizens (i.e. trade with the EU). The UK Government is introducing new legislation to ensure this is the case, so GDPR will continue to apply.

How do you define Personal Data?
Personal data is any information relating to an identifiable individual. It can identify the individual directly or indirectly (i.e. in combination with other information), so could include name, identification number, online identifier, location data, or other factors specific to the physical, genetic, mental, economic, cultural or social identity of the person.

What’s different about Sensitive Personal Data/Special Category Data?
GDPR defines a subset of personal data as Special Category Data, namely information concerning:
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Genetic or biometric data
- Physical or mental health
- Sexuality or sex life

The rules regarding Special Category Data are stricter.

How is the GDPR different from the Data Protection Act?
GDPR introduces new requirements for organisations who handle personal data, including a need to be able to demonstrate compliance to a greater extent than previously. It also establishes stronger rights for individuals designed to give them more control over how their personal data is used. It strengthens the regulatory environment and introduces enhanced penalties for non-compliance. It is intended to account for dramatic changes in the way that personal data is used, and the technological advances enabling this, that have occurred since the current Data Protection Act was introduced.
What are the GDPR principles?
GDPR contains six key principles, or golden rules, which say that personal data must be:

i) Processed lawfully, fairly and transparently.
ii) Collected for specified and legitimate purposes and not further used for other purposes incompatible with these (however, this rule is amended where the further purpose involves research).
iii) Adequate, relevant and limited to what is necessary.
iv) Accurate and kept up to date.
v) Only kept for as long as necessary for the purpose it was obtained for (however, this rule is amended where the data is being used for research).
vi) Processed in a manner ensuring appropriate security.

What does “Processing” of personal data mean?
It means any operation or set of operations that is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction.

What are the conditions for lawful processing of personal data under the GDPR?
The conditions for processing personal data are:

- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject or another person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

The conditions for processing special categories of data are:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
- Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
• Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
• Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
• Processing relates to personal data manifestly made public by the data subject
• Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
• Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
• Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
• Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
• Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

What is the difference between a Data Controller and a Data Processor?

“Data controller” means a natural or legal person, public authority, agency or any other body that, alone or jointly with other determines the purposes and means of the processing.

“Data processor”, means a natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller.

For example the University is a data controller. The companies which provide services such as storage of records or destruction of confidential records are data processors as these are performing this task/processing this data on behalf of the data controller.

What are the new rules around consent?

The GDPR sets a high bar for consent and the GDPR has been designed to give data subjects more control over how their data is used. Some of the most important elements of consent under The GDPR are:

• Consent requires a positive opt-in. The notions of having to opt-out, of pre-ticked boxes or any other method of consent by default are not allowed.
• Consent needs to be explicit.
• We need to be specific, clear and concise with regard to what people are consenting to. We need to be granular, rather than asking for blanket consent to cover a number of different things.
• Consent should not be a pre-condition of accessing a service.
People should be able to withdraw their consent at any time easily.

We need to retain records of what people have consented to, and consent should be regularly refreshed.

Can data subjects request their own data under the GDPR as they can do currently?

The GDPR contains a provision for data subjects to make a Subject Access Request, however the specifics of this are somewhat different to under the current Data Protection legislation. Currently the University can charge a fee of £10 and has 40 calendar days to provide the information. Under GDPR we can no longer charge a fee and one month to provide the information.

What other rights do data subjects have?

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

What is a Data Breach?

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just loss of personal data.

For example The University could be responsible for a personal data breach if a student record is inappropriate accessed or disclosed due to lack of internal controls, but also even if a record is retained longer than is necessary.

Does the GDPR require the University to make anyone aware when there is a breach?

The GDPR will introduce a duty on all organisations to report certain types of data breach to the Information Commissioner’s Office, and in some cases to the individuals affected.

The University will be required to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in
discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This will need to be assessed on a case by case basis. For example, we will need to notify the relevant supervisory authority about a loss of student and/or staff details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we will be required to notify those concerned directly, as well as notifying the Information Commissioner’s Office.

Under the GDPR a notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it.

Why am I being asked to complete an audit for an Information Asset Register?

Article 30 of the GDPR makes it a responsibility on organisations to maintain a record of all personal data processed by the organisation, effectively requiring an information asset register. In order for the University to create such a register it is vital that we’re able to determine what personal data is held across the University, and the legal basis that allows its processing.

What are the penalties for non-compliance with the GDPR?

Currently the Information Commissioner’s Office can fine an organisation up to £500,000 in the wake of a data breach. Under GDPR the potential fines are much higher. Depending on the nature of the offence, and which provisions of the GDPR it infringes, there are two fine structures available to the ICO.

- A fine of up to ten million euros, or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.
- A fine of up to twenty million euros, or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

What does “Data Protection by Design” mean?

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. Although not a requirement under the current Data Protection Act, this has long been championed as good practice by the ICO.

Under the GDPR, you have a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.
What is a Privacy Impact Assessment?
Privacy impact assessments (PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals’ expectations of privacy. An effective PIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and reputational damage which might otherwise occur. PIAs are an integral part of taking a privacy by design approach, and will be mandatory under the General Data Protection Regulations (GDPR) for processes and technologies that are likely to result in a high risk to the rights of data subjects.

What is the Data Classification model?
All University data has an intrinsic value and must be looked after. However, data differs widely in its sensitivity and value and, as such, in the risk that it poses. It is essential to assess the sensitivity and value of all data in order to ensure that it is handled appropriately and that the risks are effectively managed. This includes ensuring that data is stored and processed using appropriate IT facilities with appropriate security and access controls in place.

What effect will the GDPR have on research?
The biggest potential impact is centred around consent (see point 11). Consent needs to be much more informed and explicit than it is currently. The right to withdraw consent, the right to erasure and the need to refresh consent will also have an impact, however it should be noted that the new Data Protection Bill transfers the current exemption for research data that exists within the Data Protection Act 1998.

Some other aspects of the GDPR that will impact Research are the need for Privacy Impact Assessments before any research project starts, and the new requirement to notify of Data breaches within 72 hours.

What is the difference between the GDPR and the new Data Protection Bill?
The GDPR gives member states limited opportunities to make provisions for how it applies in their country. One element of the Data Protection Bill is the details of these. It is therefore important the GDPR and the Bill are read side by side.

The Data Protection Bill will also cover areas not covered by the GDPR such as Law Enforcement and National Security.