This is guidance prepared by the University of Sydney ARMS team and its intended readership is University staff. It is high level guidance only and does not take into account your specific situation. If you have any questions about how the GDPR may impact on your particular situation, please contact ARMS in the first instance. We are able to assist through the provision of guidance only. Those seeking legal advice should contact the Office of General Counsel.

ARMS guidance: General Data Protection Regulation (GDPR) and the University

What is it?
The General Data Protection Regulation (GDPR) is the new privacy law of the European Union (EU) that took effect from 25 May 2018. It applies to all EU member states.

The GDPR aims to give individuals control over their personal data and to ensure organisations implement transparent data handling practices and are accountable to individuals for the management of their personal data.

What does it cover?
The GDPR applies to controllers or processors that have establishments in the EU and who process personal data. It does not matter whether this processing takes place in the EU or not.

They GDPR also applies to the processing of personal data by controllers or processers who do not have an establishment in the EU, where they process personal data of individuals in the EU in the connection with:

- the offering of goods/services (payment is not required) or
- the monitoring of their behaviour in the EU.

What are some key features?

Lawful bases for processing personal data
The GDPR sets out six categories for the processing of personal data. For processing to be compliant at least one of the following must apply:

- consent
- contractual necessity
- legal obligation
- vital interests of the data subject
- task in public interest or
- legitimate Interest

Under the GDPR, consent is a freely given, specific, informed, unambiguous and affirmative action. This means that if you want to rely on consent as the basis for it collecting, using or disclosing personal data, you need to keep a few things in mind, including, that:

- The nature of the consent is explained clearly and simply
- The person should make a clear statement of consent
- Consent must be positive - default methods such as pre-checked box cannot be used
- Avoid making consent a pre-condition to getting a good or service.

- Obtain separate consents for different processing activities (eg. collecting and then using personal information). Blanket consent should not be used.
- It must be as easy to withdraw consent as it is to give it.

Individual rights
Under the GDPR, the individual has a number of privacy rights, including:

- erasure (also known as the right to be forgotten)
- data portability where an individual has a right to request that their data be transmitted to another party, and
- the right to object to processing.

It should be noted that there are exceptions and ways in which such rights are applied.

What does this mean for the University?
The GDPR applies to the University in specific circumstances. Examples of University activities that are affected are:

- the recruitment of students based in the EU and ongoing engagement with these students, including after graduation;
- the offering of short non-award courses to participants based in the EU;
- data analytics in relation to our students, where they are located in the EU, via such platforms as Canvas; and
- research projects that involve the monitoring of the behaviour of individuals in the EU.

What is being done in preparation for the GDPR?
The University complies with NSW privacy laws and these laws share many common requirements with the GDPR, for example:

- the information protection principles and health information principles in NSW privacy law regulate the collection, use, disclosure, secure storage, accuracy and integrity of personal information;
- NSW public agencies like the University must have transparent information handling practices, including making it clear to individuals what information they are collecting and what they will do with it; and how an individual can access and update their personal information.

There are also parts of the GDPR that do not have direct equivalents under NSW privacy laws. For example, the right to data portability. The GDPR also formalises some requirements, for example, the undertaking of privacy impact assessments (that identify and minimise non-compliance with privacy risks), that the NSW Privacy Commissioner has given clear guidance on as promoting compliance with the law.

The University is in the process of updating key privacy related documents, including collection notices for our website and students, to reflect that we are regulated by the GDPR and so that these documents meet the requirements of the GDPR.

Some key terminology

controller determines the purposes and manner in which personal information is processes
establishment can be identified where an organisation has a subsidiary, branch, school or office operating on its behalf in the EU. It can also be identified through the holding of a bank account in the EU.
monitoring refers to the tracking of an individual in order to create a profile of this individual or to somehow predict his or her behaviour or personal preferences.
personal data any information relating to an identified or identifiable natural person.
processing covers anything that can be done in relation to personal information, including automated processes, such as collection, use, disclosure, adaption, alteration, storage and destruction.
processor processes the data on behalf of the controller in accordance with the controller's instructions.