What is GDPR?
The General Data Protection Regulation comes into force 25 May 2018. It is the new legal framework that sets out the requirements for holding and using personal data and the individual’s rights in respect of that data. It replaces the Data Protection Act 1998 entirely.

What is a Data Protection Impact Assessment (DPIA)?
A Data Protection Impact Assessment details the personal data used in any process, project or system, the associated risks and their mitigation. A Data Protection Impact Assessment is mandatory for all high-volume or high-risk processing of personal data, regardless of purpose.

What is a privacy notice?
A privacy notice provides information on our use of personal data to individuals and explains why that use is fair, lawful, secure and proportionate. Privacy notices are fundamental to the University demonstrating its compliance with GDPR and acting transparently with personal data.

What do I do if I have a data incident?
Any suspected data incident must be reported to dataprotection@dundee.ac.uk immediately. The faster we are aware of any issue, the greater the opportunity to reduce the risk to individuals.

Where can I get help?
Contact t: 01382 384441 e: dataprotection@dundee.ac.uk w: dunder.ac.uk/information-governance/dataprotection

The General Data Protection Regulation (GDPR)
Students, colleagues, and partners all trust the University with their personal information. Our role as University staff is to make sure that we respect the appropriate use and security of this information. GDPR enhances our legal obligations in this domain.

Three themes underpin our compliance with GDPR

01 Security
- Use secure University systems and devices when working with personal information - do not put personal data on unsecured devices
- Avoid emailing personal data
- Lock personal data away when not in use and keep your workspace clear
- Report data incidents quickly - we only have 72 hours to respond

02 Transparency
- Tell people when and why we hold their information in privacy notices
- Respect people’s rights to access, update and/or delete personal data
- Only share data when appropriate legal and technical controls are in place (including with suppliers, system providers and research partners)

03 Responsibility
- Think ‘data protection’ whenever you work with personal information
- Use the right tools to understand and manage risks to personal data (eg DPIAs)
- Remember that you’re not on your own
- Seek support from Professional Services (Information Governance, Legal, EPDU, TASC and others)

01
02
03

The University of Dundee is a registered Scottish Charity, No. SC015096
The University and GDPR

Key questions

What is personal data?
- Data about an identified or identifiable living person
- From which they can be identified directly or indirectly
- Identification could result from a single data point, or when seemingly anonymised data points are combined
- Data points do not necessarily have to be obvious (e.g. name) to identify someone when considered in combination

What are ‘special categories’ of personal data?
- Sensitive personal data: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data; health data; sex life; sexual orientation

Why do we have personal data?
- We should understand and document why we have personal data and the purpose for which it is being used
- We should be sure that we are only holding or using the smallest amount of data needed for this purpose
- These points should be documented and communicated in privacy notices

Why is it ok for us to have personal data?
- We require personal data to fulfill many core purposes of the University
- We must know and document why our use of personal data is lawful
- This should be communicated in privacy notices
- Information Governance will help with this aspect of meeting GDPR requirements

Is personal data secure?
- We know which systems hold personal data
- We should be sure that we have implemented the right security, technical and legal controls
- If we need extra safeguards for ‘special categories’ or large volumes of personal data, they should be put in place
- If a data incident occurs, it must be reported to dataprotection@dundee.ac.uk immediately

Is access to or sharing of personal data appropriate?
- Personal data is accessed on a ‘need to know basis’
- When sharing personal data with partners, working with systems providers, implementing new systems or making disclosures, we should make sure that the sharing is appropriate and that the right controls are in place before sharing any data

Do we know how long we need personal data?
- We should check and define retention periods for our use of personal data – an institutional retention schedule is available online at dundee.ac.uk/information-governance/dataprotection
- We must understand how and when we will review and dispose of data and communicate this information in privacy notices
- If we can manage with anonymised or pseudonymised data we should dispose of personally identifiable data as soon as we can legitimately do so

Can we comply with individual’s rights?
- If someone contacts you seeking to update, access, erase, or limit the use of their information we must respond to them. If you don’t know what to do refer the query to dataprotection@dundee.ac.uk
- If we’re working with high-risk or high-volume personal data, implementing new systems or technologies, or carrying out surveillance or other potentially intrusive activities we must complete a DPIA
- We must make sure that our activities are communicated to people in ‘privacy notices’ to meet the transparency and accountability requirements in GDPR