**The EU General Data Protection Regulation (GDPR)**

## Introduction

On 25th May 2018 the GDPR will become law within the UK as we will still be full members of the EU at that point. Following the UK exit from the EU the GDPR will remain as law under the Repeal Bill until any decisions are made to change UK data protection legislation.

Many of the GDPR's main concepts and principles are much the same as those in the current data Protection Act (DPA) however there are new elements and significant enhancements so the University will need to do some things differently and make improvements in others. This reports highlights the steps we will need to take to ensure we are compliant.

## The GDPR Principles

The principles are similar to those in the DPA, with added detail at certain points and a new accountability requirement. The GDPR does not have principles relating to individuals' rights or overseas transfers of personal data - these are specifically addressed in separate articles.

The principles in Article 5 of the GDPR requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
(e) 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that
“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

The most significant addition is the accountability principle. The GDPR requires us to show how we comply with the principles – for example by documenting the decisions we take about a processing activity.

The following are the key steps we need to take to ensure compliance.

1. **Awareness**

We need to ensure that key people across the university are aware that the law is changing. We all need to appreciate the impact this will have and identify areas that could cause compliance problems under the GDPR.

To support this the new Information Governance webpages are being launched in January 2017 to support the role out of the mandatory training for all staff. A dedicated GDPR page is being built to provide guidance and advice for all staff.

2. **Information we hold**

We need to understand what personal data we hold, where it came from and who we share it with. The GDPR updates rights for a networked world, for example, if we have inaccurate personal data and have shared it with another organisation we will need to tell them so they can correct their records. An information asset register is required to document and ensure we have captured all the relevant data as well as the information asset owners so we can ensure they are aware of the changes and legally process personal data.

We will need to organise an information audit to ensure we have captured and understood what we have. This is a significant piece of work that will involve resource across the University.

3. **Communicating Privacy Information**

When we collect personal data we have to give people certain information which is usually done through a privacy notice. Under the GDPR we will be required to provide additional information and all privacy notices need to be updated.

The Information Governance team will update the privacy notices. Staff will need to ensure that any processing of personal data is covered with a privacy notice and work with the IG team to update notices accordingly.

4. **Individuals rights**

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA. Data subjects are no longer required to pay and all requests must be dealt with within one month (currently 40 days).

The GDPR provides the following rights for individuals:

1. The right to be informed – relates to the changes to privacy notices
2. The right of access – subject access requests (SAR) require additional information
3. The right to rectification – includes rectification of data shared with third parties
4. The right to erasure – deletion of personal data including shared with third parties
5. The right to restrict processing
6. The right to data portability – providing data electronically in a commonly use format
7. The right to object – includes profiling, direct marketing and processing for research
8. Rights in relation to automated decision making and profiling.

The IG team will be reviewing and implementing processes to deal with each of these rights.

All systems will need to have the ability to delete data to ensure we have the capability to comply with the right to erasure.

The Effective Learning Analytics project (and any other projects that involve automated decisions or profiling) will need to ensure full compliance and the IG team have already engaged with the ELA project on this.

## 5. Legal basis for processing personal data

All personal data must have a legal basis to enable us to process this and we need to identify what that is and ensure it is clearly explained in our privacy notices and when responding to SARs.

The GDPR includes the following conditions for processing personal data:

- Consent
- Contractual necessity
- Non-contractual legal obligations
- To protect the vital interests of the data subject
- Functions of a public nature

- Legitimate interest – public bodies can no longer use this condition

Alumni data is currently collected using the legitimate interest condition, as this will no longer be an available condition the IG team have started work with GED to ensure alumni data is legally processed.

Across the university we need to ensure we have clear understanding of the conditions we are processing personal data under and that any relevant changes are made, particularly where legitimate interest or consent is used.

## 6. Consent

The GDPR is clear when it comes to consent and the University will need to ensure where consent is used it is unambiguous, freely given, informed, specific and demonstrable. It must be a positive indication of agreement so cannot be inferred from silence, pre-ticked/opt out boxes or inactivity.

To use consent it must be freely given and can be removed so where we do use consent we must ensure we have a record of it and can remove the data should consent be withdrawn.

Work has already started between the IG team and Student Records to ensure the 2017 registration will be fully compliant with GDPR and any data collect under consent will be clear. The IG team have also engaged with the Student Guild to ensure consent is captured within the registration and data sharing between the University and the Guild is GDPR compliant.

As part of the work to understand information assets we need to identify the condition for processing and ensure any changes are made to ensure compliance. This will have significant impacts on research where we collect data and rely on consent.

## 7. Children

The GDPR brings in special protection for children's personal data and the requirement to collect parental consent. Any privacy information must be written in language that children understand.

Research, sports and any other events that include children will need to ensure compliance and work will need to be undertaken to identify where this information is being processed.

## 8. Data Breaches

The GDPR brings in mandatory reporting of personal data breaches within tight timescales and with significantly increased fines.

Serious breaches will need to be reported to the data subject and the ICO within 72 hours of identifying the breach and fines can be up to €20million.

Currently very few security incidents are reported at the University and this will need to increase, we will need to ensure all security incidents are reported quickly so that they can be investigated to identify breaches and near miss and can be contained where possible.

The new IG webpages will provide clearer information about security incidents and how to report them. We need to ensure we have the right procedures in place to detect, report and investigate any data breaches. Failure to notify a breach can also incur a fine as well as the actual data loss itself.

The majority of security incidents are caused by human error and we need to encourage staff to report these so they can be contained and information recovered where possible.

## 9. Data Protection by Design and Data Protection Impact Assessments

Under current DPA it is recommended that a Privacy Impact Assessment is carried out to ensure all projects / new systems are built with appropriate security measures and compliance with DPA. Under the GDPR this will become a legal requirement and for high-risk situations we will be required to consult with the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

Carrying out an impact assessment at the start of a project ensures privacy by design, compliance with legislation and that systems are built with security from outset and risks are

managed. This often results in better and cheaper solutions as adding in good security at a later date can be costly.

To implement this the IG team are producing template documents which include both a PIA and a risk assessment ensuring the risks are identified and relevant controls put in place. This supports the GDPR as well as information security and governance and will reduce information risk for the University.

An impact assessment is being drafted to support the ELA project.

**10. Data Protection Officer**

The GDPR has a requirement for the University to have a designated Data Protection Officer, this is currently the Information Governance Manager.

The DPO has specific duties they are required to carry out including providing advice on all GDPR issues, monitoring compliance, advising on impact assessments and being a point of contact for the ICO. Although other tasks can be carried out they must not result in a conflict of interests. The DPO reports to senior management, but they cannot instruct the DPO on role.

The University must ensure that DPO is properly and in a timely manner involved in all issues which relate to protection of personal data.

The change in law from the DPA to the GDPR will require significant changes, in particular understanding what information we have and how it's used as well as being able to demonstrate compliance. The University needs to ensure this work is given the appropriate priority to ensure compliance by May 2018.

Rhiannon Platt

Information Governance Manager