DATA PRIVACY BY DESIGN AND DEFAULT GUIDANCE

1. INTRODUCTION

The concept of data privacy by design and default is a mandatory obligation under data protection laws and aims to establish practices that ensure data protection from the outset.

Data privacy is not about preventing the University from collecting personal information as part of its role in providing services to students, employees, collaborative partners and other University stakeholders, rather it allows the maintenance of control over the collection, use, and disclosure of personal information.

The University should ensure that privacy and data protection is a key consideration in the early stages of any project and throughout its lifecycle. Examples of the types of project include:

- building or migrating to new IT systems for storing or accessing personal data;
- developing policy or strategies that have privacy implications;
- starting a data sharing initiative;
- collecting data for a new project;
- using existing data for new purposes.

2. WHY A PRIVACY BY DESIGN APPROACH?

The objectives of privacy by design are to ensure data protection and for individuals to have control over their information.

Data protection laws do not prohibit the disclosure of personal data, but any disclosure has to be in compliance with the data protection principles, that personal data shall be:

- processed fairly, lawfully and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes concerned;
- accurate and kept up-to-date;
- not kept longer than necessary for the purposes concerned;
- processed securely and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The University must also demonstrate compliance with the above principles.

A privacy by design approach is a crucial tool in limiting privacy risks and establishing trust. Designing projects, processes, products or systems with privacy considered at the outset can result in benefits which include:

- potential problems are recognised at an early stage, when addressing them will often be simpler and less costly;

- a greater awareness of privacy and data protection throughout the University;
- the University is more likely to meet its legal obligations and less likely to breach data protection laws and regulations;
- any actions are less likely to be privacy intrusive and have a negative impact on individuals.

Privacy should be proactive rather than reactive and prevent privacy invasive events prior to their occurrence.

Personal data must be protected in any given IT system or organisational practice with privacy embedded into the design and architecture of IT systems and organisational practices.

3. TECHNICAL AND ORGANISATIONAL MEASURES

The University has an obligation to implement technical and organisational measures to show that the University has considered and integrated data protection into its processing activities. Mechanisms that the University can use to limit risk and demonstrate compliance are:

(a) Data Minimisation

The technique of only processing personal data that is necessary for each specific purpose. Such measures need to ensure that personal data is not made accessible to those other than is necessary for the purpose.

(b) Aggregated Data

The process of combining information about a number of individuals into broad classes, groups or categories so that it is no longer possible to distinguish information relating to those individuals.

(c) Encryption

The process of using a secret value or 'key' that encodes data so that only users with access to that key can read the information.

(d) Anonymisation

This allows data to be placed into a form which does not identify individuals and irreversibly destroys any way of identifying those individuals.

(e) Pseudonymisation

The technique of processing personal data so that it can no longer be attributed to a specific individual without the use of additional information. The additional information must be kept separately and be subject to measures to ensure that the personal data is not attributed to an individual.

Pseudonymisation replaces identification fields within a data record by one or more artificial identifiers, or pseudonyms.

The General Data Protection Regulation defines pseudonymisation in Article 3, as:

"the processing of personal data in a way that the data can no longer be linked to discover a specific data subject without the use of further information."

(f) Data Privacy Impact Assessment (DPIA)

DPIAs can be an integral part of taking a privacy by design approach. A DPIA can assist in identifying and prioritising the next steps in managing any privacy risks.

See: Data Privacy Impact Assessment Guidance

Data Privacy Impact Assessment

DPIAs are used to:

- measure compliance with data protection laws
- identify and reduce privacy risks
- demonstrate accountability

4. FURTHER GUIDANCE

The Information Commissioner's Office (ICO) has produced guidance and codes of practice that can be found at:

Data protection by design and default:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

Anonymisation:

https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

Encryption:

https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/

Data Minimisation:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/