Abertay University

Academic Registry

Privacy by Design and by Default Policy

1. Introduction and Scope

This policy is for employees, workers and contractors of the Abertay University ("the University"). When processing personal data (defined below), Art 25 of the General Data Protection Regulation ("GDPR") obliges the University to (taking into consideration the nature of the processing, risks to individuals and costs etc,) implement appropriate technical and organisational measures, such as pseudonymisation, into such processing activities in order to meet the requirements of GDPR (including the processing principles) and protect the rights of the data subjects concerned. What are 'appropriate measures' may well change from one processing activity to the other and it is important that such measures are given consideration at the start of, and throughout, the life-cycle of the University's processing of personal data. This obligation is referred to as 'Privacy by Design'.

As a minimum, such measures must ensure that only personal data which are necessary for each specific purpose of the processing are processed and that the personal data is not made available to an indefinite amount of individuals without the data subject's involvement ("Privacy by Default").

This Policy provides guidance on the University's approach to ensuring that it embeds privacy by design and privacy by default across the University's operations.

In the event the ICO finds that the University has not met its obligations in relation to Privacy by Design and Default, the Information Commissioner's Office could potentially impose a monetary penalty of the higher of 2% of the University's annual turnover or €10M. It is therefore important that all staff understand and implement this Policy. If you have any questions, please contact the University's Governance Team in Academic Registry at foi@abertay.ac.uk .

2. Interpretation

The following definitions apply to this Policy:

Personal Data: means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Category of Personal Data: means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Criminal Conviction Data: The rules for special category personal data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures. In order to process criminal conviction data we must either:

- process the data in an official capacity; or
- meet a specific condition in Schedule 1 of the Data Protection Act 2018, and comply with the additional safeguards set out in that Act.

For the purpose of this policy, when we are referring to 'personal data', we are referring to Personal Data and Special Categories of Personal Data collectively.

Data Protection Impact Assessment (DPIA): an assessment of the impact of the envisaged processing operations on the protection of personal data as referred to under Art 35 of GDPR;

Processing Principles: means the processing principles set out in Art 5 of GDPR and as attached as an Appendix to this Policy.

Where law or regulatory policy has changed since this Policy was written, those changes shall take precedence and this Policy will be interpreted in the light of changes.

This Policy should be considered in conjunction with the guidance and forms for undertaking a DPIA, which are available on the University's intranet page for Data Protection.

A Data Protection Impact Assessment (DPIA) should be carried out where there is a high risk to individuals. This may be as part of the initial phase of a project or when an existing project is being reviewed. The DPIA should assess the risks to privacy and apply mitigation.

3. Privacy by Design – General Principles

The principles of 'Privacy by Design' can be summarised as:

1	Use **proactive** rather than reactive measures. Anticipate, identify and prevent privacy invasive events before they happen.
2	Privacy should be the **default** position. Personal data must be automatically protected in any system of business practice, with no action required by the individual to protect their privacy
3	Privacy must be **embedded** and integrated into the design of systems and business practices
4	All legitimate interests and objectives are accommodated in a **positive-sum** manner. Both privacy and security are important, and no unnecessary trade-offs need to be made to achieve both.
5	Security should be **end-to-end** throughout the entire lifecycle of the data. Data should be securely retained as needed and destroyed when no longer needed.
6	Visibility and **transparency** are maintained. Stakeholders should be assured that business practices and technologies are operating according to objectives and subject to independent verification.
7	Respect **user privacy** by keeping the interests of the individual uppermost with strong privacy defaults, appropriate notice and user friendly options.

4. Technical and Organisational Measures

The University's aim is to implement appropriate technical and organisational measures which are designed:

(a) to implement the Data Protection Principles in an effective manner, and
(b) to integrate into the processing of personal data the safeguards necessary for that purpose.

This Policy applies at the time of determining the means of processing, and at the time of actually processing the personal data.

In doing so, the University will take into account the available technical and organisational measures, the cost of implementation and the nature, scope, context and purposes of processing of personal data, as well as the risks of varying likelihood and severity for rights and freedoms of individuals presented by the processing of their personal data.

If it is considered that the processing presents a **high risk** to individuals, a DPIA must be carried out in accordance with the University's procedures found on the Data Protection intranet page.

5. Privacy By Default

The University's aim is that appropriate technical and organisational measures will be applied to ensure that, by default, only the personal data which is necessary for each specific purpose of processing of personal data is used, in relation to:

(a) the amount of personal data collected;
(b) the extent of processing that personal data;
(c) the period of its storage; and
(d) its accessibility.

The University's aim is that by default personal data should be restricted to those who have a business need to know.

6. Data Protection by Design

The University's aim is that when considering a proposal for a particular type of processing of personal data, the impact of this on the individuals affected should be considered, and that appropriate technical and organisational measures should be put into place to ensure that:

(a) the Data Protection Principles are implemented; and
(b) any risks to individuals' rights and freedoms are minimised.

Vigilance by staff should be exercised continually to ensure the security of University systems and personal data, e.g. against attempts to trick individuals into revealing their log-in details; and to avoid risks of personal data breaches arising from mobile devices and remote log-ins. Staff should avoid downloading, working with or storing identifiable personal data wherever possible, and only undertake these activities in compliance with appropriate University guidance and policies. Anonymised or partly/reversibly anonymised data should be used wherever possible.

When buying systems/software which involve personal data, or considering transfers/sharing of personal data including using the "cloud", staff must evaluate the privacy and security of alternative solutions and vendors/partners. The use of such systems/software should to the maximum extent possible avoid personal data being involved or put at risk of a data breach. Personal data should only be placed on systems, devices or software where this is compliant with University policies and the legislation. The use, and duration of holding, of personal data should be minimised.

Reviews of, and improvements to, privacy should be undertaken regularly by staff in their areas of work, documented, and privacy risks and precautions reviewed by staff regularly. Further information is available on the University's intranet.

Managers or staff should not purchase new systems or software without first reviewing their proposed use in terms of a Data Protection Impact Assessment if the proposed use presents a high risk to individuals, and the proposed purchase also requires to be checked first by Procurement and by Information Services for contract terms, and for the uses of, and risks to, personal data.

For purchasing supplies/services, regardless of contract value, no managers or staff should approve a contract with a supplier unless the terms have been checked by Procurement (or the University's Solicitors) for data protection compliance.

7. Examples of Risk Mitigation Techniques

Non-exhaustive examples of techniques which may be used to achieve these aims include undertaking University-required data protection training and refresher training modules; maintaining awareness of data security and threats such as 'phishing' attacks and other scams; carefully considering email recipients, and avoiding emails to multiple recipients wherever possible; avoiding the storage of spreadsheets containing personal data (anonymise and delete after use) minimisation of collecting, storing, using and transmitting personal data used; regular deletion of personal data after completion of purpose of processing or retention period; full and irreversible anonymisation of personal data; regular checks to ensure personal data accuracy; pseudonymisation; encryption e.g. of spreadsheets and other documents; filing personal data in University drives rather than using Outlook as a storage medium; ensuring transparency for data subjects by Privacy Notice; restricting staff access to personal data to those with a need to know; .

Another potential technique which may be helpful, provided that the number of individuals in the dataset is large enough, may be to generate a dataset composed entirely of identity-disguised or 'fictional' individuals which can retain the statistical properties of the original dataset.

Appendix

Article 5: Principles relating to processing of personal data

1.Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

(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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(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 (‘accuracy’);

(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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

(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 (‘integrity and confidentiality’).

2.The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).