Data Protection Policy

Table of Contents

1. INTRODUCTION 2
2. REFERENCE DOCUMENTS 2
3. PURPOSE 2
4. SCOPE 2
5. PRINCIPLES 3
6. DATA SUBJECT RIGHTS 3
7. DATA BREACHES 4
8. DATA TRANSFERS 4
9. ROLES AND RESPONSIBILITIES 4
10. VALIDITY AND DOCUMENT MANAGEMENT 5

1. Introduction

The Institute of Public Administration ("the Institute" or "the IPA") processes the personal data of students, staff members and third parties in the course of carrying out its various functions. This processing is governed by the EU General Data Protection Regulation (GDPR) and the Data Protection Act (2018) (collectively: "the legislation").

2. Reference Documents

- EU General Data Protection Regulation 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Data Protection Act, 2018 (DPA)
- Information Security Policy
- Data Breach Policy
- Data Management and Retention Policy

3. Purpose

The purpose of this Data Protection Policy is to advise staff, students and other members of the Institute's community of their responsibilities regarding the handling of Personal Data and Special Categories of Personal Data as set out in Irish and European Law.

4. Scope

This policy provides a framework for ensuring that the Institute meets its obligations under the legislation.

It applies to all processing of personal data carried out by or on behalf of the Institute, irrespective of whether the data is processed on Institute or non-Institute equipment or by third parties, and irrespective of whether the processing takes place on Institute premises or remotely.

'Personal data' means any information relating to an identifiable living individual who can be identified from that data or from that data and other data.

'Processing' means anything that is done with personal data, including collection, storage, use, disclosure and deletion.

More stringent conditions apply to the processing of special-category personal data.

'Special category' 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 to uniquely identify an individual, data concerning health or data concerning an individual's sexual life or orientation.

This policy should be read in conjunction with the Reference Documents outlined at 2 above, as well as any other documents that impose confidentiality or data management obligations in respect of information held by the Institute.

This policy does not cover the use of personal data by members of the Institute when acting in a private or non-Institute capacity.

5. Principles

The processing of personal data must comply with data protection legislation and the principles of data protection.

In summary, these require that personal data be:

- processed fairly, lawfully and transparently.
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- adequate, relevant, and limited to what is necessary.
- accurate and, where necessary, up to date.
- not kept for longer than necessary; and
- kept safe and secure.

In addition, the principle of accountability requires that the Institute can evidence compliance with these principles.

6. Data Subject Rights

Data Subjects' Rights are enshrined in the legislation. The IPA is committed to upholding these rights and will respond to all rights requests by the legislation. Detailed guidance and support on upholding individuals' rights is available from the Data Protection Officer. The rights of the data subject are:

- The right to be informed: Individuals should be informed about the processing of their data. There are specific provisions set out under data protection law regarding the information which should be provided to individuals (usually via a privacy notice) when collecting personal data.
- The right of access: Individuals have the right to make an access request for a copy of their data and to exercise that right easily and at reasonable intervals.
- The right to rectification: Individuals have the right to have inaccurate personal data about them rectified.
- The right to erasure: This is also known as the 'right to be forgotten'. Individuals have the right, under certain circumstances, to have their data erased.
- The right to restrict processing: Individuals have the right, under certain circumstances, to request the restriction of processing of their data.

- The right to data portability: In the case of electronic data, individuals have the right to have their data transferred to another data controller electronically so that the data can be processed on different platforms and services, under certain circumstances.
- The right to object to processing: Individuals have the right, under certain circumstances, to object to processing their data.
- Automated individual decision-making: Individuals have the right to be informed about the existence of automated individual decision-making concerning their data.

These rights are not absolute and are subject to certain exemptions under data protection legislation. Additional information and guidance are available from the Institute's Data Protection Officer.

7. Data Breaches

Where a breach concerning personal data takes place the Institute's Data Breach Policy must be followed. In particular, the individual discovering or suspecting the breach must inform their manager and the Data Protection Officer as soon as possible so that the appropriate action is taken.

8. Data Transfers

Personal data may be transferred within the European Union and the European Economic Area (EU member states plus Norway, Iceland and Liechtenstein).
Any proposed transfer of personal data outside the EU/EEA must be notified in advance to the Data Protection Officer so that the appropriate safeguards are put in place.

9. Responsibilities

Responsibility

IPA has overall responsibility for ensuring compliance with Data Protection legislation when it is the Data Controller of personal data. However, all employees and students of IPA who separately collect and/or control the content and use of personal data are individually responsible for compliance with the legislation. The Institute Data Protection Officer provides support, assistance, advice, and training to all departments and offices to ensure that they can comply with the legislation.

All users of the IPA information:

Must complete relevant ongoing training and awareness activities provided by the Institute to support compliance with this policy.

- Should take all necessary steps to ensure that no breaches of information security result from their actions.

- Must report all suspected and actual data security breaches to their head of area /function who must in turn report the incident immediately to the Information the DPO cc'ing the Director General, so that appropriate action can be taken to minimise harm.

- Must inform the Institute of any changes to the information that they have provided to them in connection with their employment or studies (e.g., changes of address or bank account details).

10. Validity and document management

This document is valid as of 08th May 2023

The owner of this document is the Director General, who will check and, if necessary, update the document at least annually.