CENTRAL APPLICATIONS OFFICE

DATA PROTECTION POLICY

CAO
www.cao.ie

Contents

1. Introduction

The Central Applications Office (hereafter referred to as "CAO") is committed to protecting the rights and freedoms of our data subjects, and safely and securely processing their data in accordance with all of our legal obligations, including compliance with the General Data Protection Regulation (GDPR).

We process both personal and sensitive data about our employees, applicants, suppliers, and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our employees, joint controllers and third-party data processors understand the rules governing their use of the personal data to which they have access during the course of their work on behalf of CAO.

2. Scope

This policy applies to all personal data processed by the CAO. The CAO and any Higher Education Institution (hereafter referred to as "HEI") you apply to are considered to be Joint Controllers of the personal data related to the application and therefore will have access to the data.

All personal and sensitive data will be equally referred to as personal data in this policy, unless specifically stated otherwise.

This policy supplements other CAO policies relating to data protection, and email and systems use. Those policies including *inter alia*:

- ICT Policy
- Data Breach Management Policy
- Data Retention Policy
- Subject Access Request Policy

The CAO may supplement or amend this policy by additional policies and guidelines.

3. Principles of the General Data Protection Regulation

The following outlines the principles of the General Data Protection Regulation. The CAO is required to adhere to the principles set out below.

3.1. *Lawfulness, Fairness and Transparency*

All data must be processed legally, and in a way that is fair and transparent. The Data Subject will be clearly informed about how their data is being processed at the time it is being captured and who their data is shared with. The Data Subject's data will not be shared with or disclosed to a third party other than to a party contracted to CAO and operating on its behalf.

A Data Transparency Policy document is available to view on the website and can be used to explain to data subjects why and how their data is being processed.

3.2. *Collected for specific, explicit and legitimate purposes*

CAO will only collect data from data subjects for a specific purpose, and this purpose will be made clear to the data subject at the time the data is collected.

Once data is collected for a specific purpose, it will not be processed for any other purpose without the data subject's prior consent.

3.3. *Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*

CAO will ensure that any data obtained from the data subject will be adequate and relevant to the purpose(s) for which it is being processed. No unnecessary or additional data will be processed if the original purpose has been satisfied.

3.4. *Accurate and, where necessary, kept up-to-date*

Every effort will be made to ensure that all data collected from data subjects is accurate. Data held on the CAO system will be updated periodically to ensure any inaccuracies are rectified. Where CAO is made aware of any inaccurate data by the data subject, we will rectify this immediately. CAO will ensure that any out-of-date data be destroyed or deleted.

It may not be possible to rectify inaccurate due to assessment procedures.

3.5. *Kept in a form which permits identification of data subjects for no longer than is necessary*

Data will be retained for no longer than is necessary in light of the purposes for which that data was originally collected and processed. Any unsolicited data received by CAO employees, via email or post, will be deleted/destroyed immediately.

The CAO Data Retention Policy is available to view on the website and CAO staff should familiarise themselves with the content of the policy.

3.6. *Processed in a manner that ensures appropriate security of personal data*

All data will be processed safely and securely, to prevent unlawful or unauthorised processing, accidental or unlawful destruction, or accidental loss or damage to the data.

CAO will conduct a periodic security review of its IT systems to ensure that the appropriate measures are in place and adhered to.

3.7. *Accountability for the implementation of the above principles*

As a Data Controller, CAO takes responsibility to adhere to the above principles at all times during the course of business. CAO will keep a record of all personal data collected, held or processed. The following details will be recorded:

- The name and contact details of the Controller, and where applicable, the Joint Controller and Data Protection Officer
- The purposes of the processing
- Categories of data subjects and personal data
- Categories of recipients/third parties with whom the data will be shared
- Retention periods for each category of data
- Transfers of data to other countries
- Details of the technical/security measures in place

If, during any stage of data processing, a CAO employee/Data Processor is unsure of their obligations under the above GDPR principles, they should contact the DPO for clarification.

4. Data Protection Officer

As part of the General Data Protection Regulation, it is mandatory for CAO to have a formally appointed Data Protection Officer ("DPO").

The DPO will be included in any matters involving data protection at the earliest possible stage, including privacy impact assessments, data processing activities that may affect data subjects, and incidents which affect the data of subjects.

4.1. Responsibilities of the DPO

The DPO will be responsible for the following:

- To inform and advise CAO, its employees, and third-party data processors of their obligations under the GDPR;
- To monitor compliance with GDPR and CAO policies in relation to the protection of personal data, including raising awareness of these policies amongst CAO employees, ensuring relevant and continuous staff training, and auditing and reviewing CAO systems and procedures;
- To act as the contact point with the supervisory authority on issues relating to CAO's processing activities;
- To ensure a strict code of confidentiality concerning their role as DPO;
- To provide advice to CAO, where requested, regarding Data Privacy Impact Assessments and to monitor their performance.

4.2. Contacting the DPO

The contact details of the DPO will be published on the CAO website.

The DPO should be notified of data breaches as per joint controller agreements, processor agreements or as per data breach management policy.

5. Subject Access Requests

In order to submit a subject access request please refer to the data privacy section of the CAO website.

6. Data Protection Breach

6.1. What is a personal data breach?
A personal data breach is described as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

6.2. Reporting a breach
The CAO treats data breaches very seriously. The DPO should be notified of data breaches as per joint controller agreements, processor agreements or as per data breach management policy.

A record of any data breach that occurs, including a description of the breach, its effects and the remedial action taken, will be kept in the CAO Data Breach Log.

Where the personal data breach results in a high risk to the rights and freedoms of a data subject, the CAO are obliged to inform the data subject immediately.

6.3. Data Breach Management Policy
In the event of a data breach occurring, the CAO's '*Data Breach Management Policy*' outlines the procedure to be followed in responding to and managing the breach.

7. Training, Auditing & Monitoring

7.1. Training
All CAO employees will receive data protection training specific to their role. This training will be periodically reviewed and refreshed to ensure continuing professional development in the area of data protection law and the general data protection regulation.

7.2. Auditing & Monitoring
Methods of collecting, holding and processing personal data will be regularly evaluated and reviewed. All employees, joint controllers and third-party processors working on behalf of CAO will be made fully aware of both their individual responsibilities and CAO's responsibilities under the Regulation and under this Policy.

8. Glossary

Personal Data	'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.
Data Subject	An individual who is the subject of the personal data.
Special Categories of Personal Data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information — any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data Controller	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data Processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Joint Controller	Joint Controllers as defined in Article 26 of the GDPR jointly determine the purposes and means of processing of personal data.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory Authority	This is the national body responsible for data protection. The supervisory authority for our organisation is the Data Protection Commission.