Irish Countrywomen's Association
Bantracht na Tuaithe

Data Protection Policy

Contents

1. **Introduction**
2. **Rationale**
3. **Scope**
4. **Definitions**
    - A. *Data*
    - B. *Personal Data*
    - C. *Sensitive Personal Data*
    - D. *Automated Data*
    - E. *Manual Data*
    - F. *Data Controller*
    - G. *Data Subject*
    - H. *Data Processor*
    - I. *Data Protection*
    - J. *Data Protection Officer*
    - K. *Relevant Filing System*
5. **ICA as a Data Controller**
    - A. *Subject Access Requests*
    - B. *Third party Processors*
6. **Data Protection Principles**
7. **Data Subject Access Requests**
8. **Implementation**
9. **Security**
10. **Summary**

1. Introduction

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of the ICA (The Irish Countrywomen 's Association). This includes obligations in dealing with Personal Data, in order to ensure that the organisation complies with the requirements of the relevant Irish and European legislation, namely the Universal Declaration of Human Rights (1948), the Constitution of Ireland (1937), the Data Protection Act (1998), the Data Protection (Amendment) Act (2003), the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations (2011)) and the European General Data Protection Regulation (EU) 2016/679.

2. Rationale

The ICA, as an organisation that collects, stores and processes data about living people on computers and in a structured filing system must comply with the Data Protection principles set out in the relevant Irish & EU and European legislation. This Policy applies to all Personal Data collected, processed and stored by the ICA in relation to its staff and employees, members, service suppliers, donors, directors, trustees, other officers and stakeholders during its activities.

3. Scope

This Policy covers only Personal Data held in relation to Data Subjects by the ICA. The ICA does not collect Sensitive Personal Data. The Policy applies equally to Personal Data held in manual and automated form. All Personal Data will be treated with care by the ICA.

This policy should be read in conjunction with the associated policy and procedure documents:

I. *Data Subject Request Policy*
II. *Personal Data Breach Notification Policy and relevant notification of personal data breach templates to:*
   a. *Supervisory Authority;*
   b. *Data Controller;*
   c. *Data Subject.*
III. *Third Party Processing Policy*
IV. *Social Media Policy.*

4. Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions apply within this Policy:

I. Data

Means information in a form which can be processed. It includes both automated data and manual data.

II. Automated Data

Means information that a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, or b) is recorded with the intention that it should be processed by means of such equipment.

III. Manual Data

Means information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system

IV. 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.

'*Genetic data*' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

'*Data concerning health*' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

The ICA uses and holds personal data information for the purposes to communicate with current members, current donors and potential ones, current and former volunteers, current and former employees and/or staff members, current and former directors and trustees, current and former shareholders, and current and former service suppliers, as well as for the purpose of processing payments and/or donations.

V. Special Category Personal Data

This relates to specific categories of sensitive data which are defined as data relating to a person's ethnic or racial origin, political opinions, religious or other beliefs, trade union membership, and genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. The processing of Special Categories of Persona Data shall be prohibited under Art. 9 of GDPR – exceptions provided by regulation are not relevant to the work of the ICA.

The ICA presently does not and continues not to keep information relating to a person's sensitive data. If in the future the organisation were to keep information relating to a person's sensitive data, the ICA will only collect it when it's strictly necessary, requesting the person's consent and will handle this data with care and discretion. An amendment will be noted in this policy.

VI. Data Controller

Person(s) or entity that controls the contents and use of Personal Data: this 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

The ICA is a Data Controller.

**The Data Protection Acts require certain Data Controllers to register with the Data Protection Commissioner, however as the ICA is an organisation not established or conducted for profit and process data only related to our members and supporters and our activities, is exempted from registration.*

VII. Data Subject

A living individual who is the subject of Personal Data, i.e. to whom the data relates either directly or indirectly.

The ICA's staff and employees, members, service suppliers, donors, volunteers, employees of Trusts/Foundations and Institutional funders, its directors and trustees, and stakeholders are Data Subjects.

VIII. Data Processor

A person who processes Personal Data on behalf of a data controller, other than an employee of a data controller who processes such data in the course of their employment.

IX. Data Protection

It is the means by which the privacy rights of individuals are safeguarded in relation to the processing of their Personal Data. The Data Protection Acts 1988 and 2003 and the General Data Protection Regulation (EU) 2016/679 confer rights on individuals as well as placing responsibilities on those persons processing Personal Data.

X. Data Protection Officer

A person appointed by the ICA to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from Data Subjects and the Data Protection Commissioner.

Art. 37 of the General Data Protection Regulation (EU) 2016/679 requires that the controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

Under GDPR, the ICA is not required to name/appoint a Data Protection Officer (DPO).

The requirement to appoint a DPO should be reviewed yearly or should the circumstances of the organisation and its data processing purposes change in line with restrictions applied by the regulation.

XI. Relevant Filing System

Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable or accessible.

GDPR further extends on the meaning of '*filing system'* as any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

5. The ICA as a Data Controller

In the course of its daily organisational activities, The ICA acquires, processes and stores Personal Data in relation to:

- Members.
- Staff and Employees.
- Directors and/or Trustees.
- Volunteers.

The ICA currently does not engage third party service suppliers which requires to acquire, process and store Personal Data.

In accordance with Irish & EU Data Protection legislation, this data must be acquired and managed fairly.

Not all the ICA's staff members will be expected to be experts in Data Protection legislation. However, the ICA is committed to ensuring that all staff have sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the ICA's relevant policies and procedures are followed, in order that appropriate corrective action is taken.

I. Subject Access Requests

The ICA has prepared a Data Subject Access Request Policy to ensure correct handling of all requests.

Data Subjects are entitled to request access to any information held about them, which includes Personal Data. Any valid, formal, written request by a Data Subject for a copy of their Personal Data (a Subject Access Request) will be referred, as soon as possible, to the relevant staff member. If valid, a response including copies of the held information will be given to the Data Subject within 30 calendar

days. It is intended that by complying with these guidelines, the ICA will adhere to best practice regarding the applicable Data Protection legislation.

II. Third party Processors

In the course of its role as Data Controller, the ICA may engage Data Processors to process Personal Data on its behalf.

In each case, a formal, agreement is in place with the Processor, outlining their obligations in relation to the Personal Data, the specific purpose or purposes for which they are engaged, and the understanding that they will process the data in compliance with the Irish & EU Data Protection legislation.

6. Data Protection Principles

The following key principles are enshrined in Irish & EU legislation and are fundamental to the ICA's Data Protection policy.

In its capacity as Data Controller, the organisation ensures that all data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

For data to be obtained fairly, the Data Subject will, at the time the data is being collected, be made aware of:

- The identity of the Data Controller (the ICA).
- The purpose(s) for which the data is being collected.
- The person(s) to whom the data may be disclosed by the Data Controller.
- Any other information that is necessary so that the processing may be fair.

The ICA will meet this obligation in the following way.

- Where possible, the informed consent of the Data Subject will be sought before their data is processed;
- Where it is not possible to seek consent, the ICA will ensure that collection of the data is justified under one of the other lawful processing conditions – legitimate interest, legal obligation, contractual necessity, etc.;
- Where the ICA intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view;

- Processing of the Personal Data will be carried out only as part of The ICA's lawful activities, and it will safeguard the rights and freedoms of the Data Subject;
- The Data Subject's data will not be disclosed to a third party other than to a party contracted to the ICA and operating on its behalf, or where The ICA is required to do so by law or by an appropriate regulator.

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The ICA will obtain data for purposes which are specific, lawful and clearly stated. A Data Subject will have the right to question the purpose(s) for which the ICA holds their data, and it will be able to clearly state that purpose or purposes.

Any use of the data by the ICA will be compatible with the purposes for which the data was acquired.

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

The ICA will ensure that the data it processes in relation to Data Subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

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').

The ICA will:

1. Ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;
2. Conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date.
3. Conduct regular assessments in order to establish the need to keep certain Personal Data.

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 (storage limitation).

The ICA will define matrix of data categories, with reference to the appropriate data retention period for each category. The matrix will apply to data in both a manual and automated format.

Once the respective retention period has elapsed, the ICA undertakes to destroy, erase or otherwise put this data beyond use.

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')

The ICA will employ high standards of security in order to protect the Personal Data under its care.

Access to and management of staff and members' records is limited to those staff members who have appropriate authorisation.

g. managed and stored in such a manner that, in the event a Data Subject submits a valid Subject Access Request seeking a copy of their Personal Data, this data can be readily retrieved and provided to them.

The ICA has implemented a Subject Access Request Policy by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

7. Data Subject Access Requests

As part of the day-to-day operation of the organisation, the ICA's staff engages in active and regular exchanges of information with Data Subjects. Where a valid, formal, written request is submitted by a Data Subject in relation to the data held by the ICA, such a request gives rise to access rights in favour of the Data Subject.

In accordance with the relevant regulation, the ICA will not apply a charge in order to process such requests.

There are specific timelines within which the ICA must respond to the Data Subject, depending on the nature and extent of the request. These are outlined in the attached Data Subject Access Request policy.

The ICA's staff will ensure that, where necessary, such requests are forwarded to the relevant staff member in a timely manner, and they are processed as quickly and efficiently as possible, but within not more than 30 calendar days from receipt of the request.

8. Implementation

As a Data Controller, the ICA ensures that any entity which processes Personal/Organisational Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation.

Failure of the ICA's staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

9. Security

All possible measures - technical and organisational shall be taken against unauthorised or unlawful processing of personal data and/or against accidental loss or destruction of, or damage to, personal data. In practice, this means the ICA will deploy appropriate security to prevent the personal data from being accidentally or deliberately compromised. In particular, in cases in which the ICA will require third party providers, jointly will:

- design and organise security to fit the nature of the personal data that The ICA hold and the harm that could result from a security breach;
- be clear about who in the organisation is responsible for ensuring information security;
- make sure it has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

Summary Statement

The ICA's Data Protection Policy is a statement of the organisation's commitment to protect the rights and privacy of individuals (Data Subjects) in accordance with Irish and European Data Protection Laws and Regulations.

The ICA has developed relevant policies and procedures to accompany this document so as to ensure that the ICA is compliant with regulatory requirements, open and transparent with our members s so that the need for us to collect and hold specific data is clearly understood, and thus provide assurance around its processing, use and security.

This Data Protection Policy is augmented by the following policy and procedure documents, as noted in pt.3:

I. Data Subject Request Policy

II. Personal Data Breach Notification Policy and relevant notification of personal data breach templates to:

a) Supervisory Authority;

b) Data Controller;

c) Data Subject.

III. Third Party Processing Policy

IV. Social Media Policy.

The ICA will review this policy on an annual basis and reserves the right to submit required changes to Trustees for final approval when needed.