Irish Countrywomen's Association
Bantracht na Tuaithe

Personal Data Breach (PDB) Notification Policy

1. Introduction:

This policy sets out the policies and procedures of The Irish Countrywomen's Association (ICA) with respect to detection of personal data breaches, responding to personal data breaches and notification of personal data breaches to supervisory authorities, data controllers, data subjects and relevant others.

When dealing with personal data breaches, the ICA and staff will focus on protecting individuals (Data Subjects / DS) and their personal data (PD), as well as protecting the interests of the ICA.

2. Definitions:

In this policy:
(a) **"appointed person"** shall mean the individual primarily responsible for dealing with personal data breaches affecting the ICA.

(b) "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;

(c) "data processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

(d) "data subject" means an identified or identifiable natural person; 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;

(e) "personal data" means any information relating to an identified or identifiable natural person ('data subject');

(f) "personal data breach" means 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;

(g) "supervisory authority" means the Data Protection Commissioners' Office for the Republic of Ireland (www.dataprotection.ie);

3. Detection of personal data breaches

3.1 The ICA has put in place technological measures to detect incidents which may result in personal data breaches. As at the date of this policy, those measures include both control factors that reduce the risk of a data breach and the appointment of a third-party expert IT service company data controller who acts on our behalf to control and protect personal data whilst applying the most up to date technological tools in order to secure and/or detect a data breach.

3.2 The ICA has in place organisational measures to detect incidents which may result in personal data breaches. Adherence to various levels of authority in regard to access to data, amendment of data, and transfer of data are part and parcel of a preventative measure that enables detection. All interaction with personal data on The ICA systems is logged. Access to data in the first instance requires the individual processor to have authority and password protected access.

3.3 The ICA shall regularly review the technical and organisational measures it uses to detect incidents which may result in a personal data breach. Such reviews shall be carried out on an annual basis.

4. Responding to personal data breaches

4.1 All the ICA personnel and relevant staff in the third-party company providing IT services must notify the appointed person and/or the CEO of the ICA immediately if they become aware of any actual or possible personal data breach.

4.2 The appointed person is primarily responsible for investigating possible and actual personal data breaches and for determining whether any notification obligations apply. Where notification obligations apply, the appointed person is responsible for notifying the relevant third parties in accordance with this policy.

4.3 All personnel of the company must cooperate with the appointed person in relation to the investigation and notification of personal data breaches.

4.4 The appointed person must determine whether the ICA is acting as a data controller and/or a data processor with respect to each category of personal data that is subject to a personal data breach. the ICA is likely to act as:

4.4.1 Data controller in relation to the following categories of personal data:

4.4.1.1 *Listed separately in Third Party I.T. agreement.*

4.4.2 Data processor in relation to the following categories of personal data:

4.4.2.1 *Listed separately in Third Party I.T. agreement.*

4.5 The steps to be taken by the appointed person when responding to a personal data breach may include:

4.5.1 Ensuring that the personal data breach is contained as soon as possible;

4.5.2 Assessing the level of risk to data subjects as soon as possible;

4.5.3 Gathering and collating information from all relevant sources;

4.5.4 Considering relevant data protection impact assessments;

4.5.5 Informing all interested persons within the ICA and any third party service company of the personal data breach and the investigation, including any other relevant stakeholders;

4.5.6 Assessing the level of risk to the ICA;

4.5.7 Notifying supervisory authorities, data controllers, data subjects and others of the breach in accordance with this policy;

4.6 The appointed person shall keep a full record of the response of the ICA to a personal data breach, including the facts relating to the personal data breach. Its effects and the remedial action taken. This record shall form part of the ICA personal data breach incident file and register.

5. Notification to supervisory authority

5.1 This section 5 applies to personal data breaches affecting personal data with respect to which the ICA is acting as a data controller.

5.2 The ICA must notify the supervisory authority of any personal data breach to which this section 5 applies without undue delay and, where feasible, not later than 72 hours after the company becomes aware of the breach, save as set out in subsection 5.4.

5.3 Personal data breach notifications to the supervisory authority must be made by the appointed person using the form set out in Schedule 1 (Notification of Personal Data breach to supervisory authority).

5.4 The ICA will not notify the supervisory authority of a personal data breach where the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The appointed person shall be responsible for determining whether this sub-section 5.4 applies, and the appointed person must create a record of any decision not to notify the supervisory authority. This record should include the appointed person's reasons for believing that the breach is unlikely to result in a risk to the rights and freedoms of natural person(s). This record shall be stored as part of the personal data breach incident file and register.

5.5 To the extent that the ICA is not able to provide to the supervisory authority all the information specified in Schedule 1 (Notification of Personal Data breach to supervisory authority) at time of the initial notification the ICA must make all reasonable efforts to ascertain the missing information. That information must be provided to the supervisory authority, by the appointed person, as and when it becomes available. The appointed person must create a record of the reasons for any delayed notification under this sub-section 5.5. This record shall be stored as part of the personal data breach incident file and register.

5.6 The ICA must keep the supervisory authority informed of changes in the facts ascertained by the ICA which affect any notification made under this section 5.

6. Notification of personal data breach to data controller

6.1 This section 6 applies to personal data breaches affecting personal data with respect to which the ICA is acting as a data processor.

6.2 The ICA must notify the affected data controller(s) of any personal data breach to which this section 6 applies without undue delay and where feasible, not later than 36 hours after the ICA becomes aware of the breach. In addition, the ICA must comply with the provisions of the contract(s) with the affected data controller(s) relating to such notifications.

6.3 Personal data breach notifications to the affected data controller(s) must be made by the appointed person using the form set out in Schedule 2 (Notification of personal data breach to data controller). The completed form must be sent to the affected data controller(s) by secure and confidential means. The appointed person must keep a record of all notifications and all other

communications with the affected data controllers relating to the breach, as part of the personal data breach incident file and register.

6.4 To the extent that the ICA is not able to provide to the affected data controller(s) all the information specified in Schedule 2 (Notification of Personal Data breach to data controller) at time of the initial notification the ICA must make all reasonable efforts to ascertain the missing information. That information must be provided to the affected data controller(s), by the appointed person, as and when it becomes available. These notifications shall be stored as part of the personal data breach incident file and register.

7. Notification of personal data breach to data subject(s)

7.1 This section 7 applies to personal data breaches affecting personal data with respect to which the ICA is acting as a data controller.

7.2 Notifications to data subject under this section 7 should, where appropriate, be made in consultation with the supervisory authority and in accordance with any guidance given by the supervisory authority with respect to such notifications.

7.3 The ICA must notify the affected data subject of any personal data breach to which this section 7 applies if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, save as set out in sub-section 7.5.

7.4 Personal data breach notifications to the affected data subjects must be made by the appointed person in clear and plain language using the form set out in Schedule 3 (Notification of personal data breach to data subject). The completed form must be sent to the affected data subject(s) by appropriate means. The appointed person must keep a record of all notifications and all other communications with the affected data subjects relating to the breach, as part of the personal data breach incident file and register.

7.5 The ICA has no obligation to notify the affected data subject of personal data breach if:

7.5.1 the ICA has implemented appropriate technical and organisational protection measures (in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption), and those measures have been applied to the personal data affected by the personal data breach;

7.5.2 The ICA has taken subsequent measures which ensure that a high risk to the rights and freedoms of data subjects is no longer likely to materialise;

7.5.3 It would involve disproportionate effort (in which case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner), providing that the appointed person shall be responsible for determining whether this sub-section 7.5 applies, and the appointed person must create a record of any decision not to notify the affected data subjects. This record should include the appointed person's reasons for believing that the breach does not need to be notified to the affected data subjects. This record shall be stored as part of the personal data breach incident file and register.

7.6 If the ICA is not required by this section 7 to notify affected data subjects of a personal data breach, the ICA may nonetheless do so where such notification is in the interests of the company and/or the affected data subjects.

8. Other notifications

8.1 Without affecting the notification obligations set out elsewhere in this policy, the appointed person should also consider whether to notify any other third party of a personal data breach. Notifications may also be required under law or under an agreement, or terms of reference (project) or contract. Relevant third parties may include: Donors, Funders, Sponsors, Foundations, Trusts, partners or the Charities Regulator, to name a few.

9. Notification Schedules

9.1 Schedule 1 - Notification of personal data breach to supervisory authority

a. Introduction: *identification of person giving personal data breach notification.*
b. Description of personal data breach: *general description of personal data breach*.
c. Categories of data subject affected: *categories of data subject affected.*
d. Number of data subjects affected: *number of data subjects affected.*
e. Categories of personal data concerned: *categories of personal data concerned.*
f. Number of records concerned: *number of records concerned.*
g. Likely consequences of breach: *likely consequences of personal data breach.*
h. Measures taken to address breach: *measures taken to address breach.*
i. Has breach been notified to data subjects: *details of whether data breach notified to data subjects?*
j. Late reporting of breach: *reasons for late report by controller of personal data breach.*
k. Contact details: *contact details for the ICA person handling the personal data breach.*

9.2 Schedule 2 - Notification of personal data breach to data controller

a. Introduction: *identification of person giving personal data breach notification.*
b. Description of personal data breach: *general description of personal data breach.*
c. Categories of data subject affected: *categories of data subject affected.*
d. Number of data subjects affected: *number of data subjects affected.*
e. Categories of personal data concerned: *categories of personal data concerned.*
f. Number of records concerned: *number of records concerned.*
g. Likely consequences of breach: *likely consequences of personal data breach.*
h. Measures taken to address breach: *measures taken to address breach.*
i. Contact details: *contact details for the ICA person handling the for personal data breach.*

9.3 Schedule 3 - Notification of personal data breach to data subject

a. Introduction: *identification of person giving personal data breach notification.*
b. Description of personal data breach: *general description of personal data breach:*
c. Categories of personal data concerned: *categories of personal data concerned.*
d. Likely consequences of breach: *likely consequences of personal data breach.*
e. Measures taken to address breach: *measures taken to address breach.*
f. Steps to mitigate breach: *steps data subject may take to mitigate personal data breach.*
g. Contact details: *contact details for the ICA person handling the personal data breach.*