Irish Countrywomen's Association
Bantracht na Tuaithe

Third Party Processing Policy

1. Purpose

This policy sets out our procedures for the safe handling of personal data that is processed on our behalf by external agents (Data Processors), should the need arise. The Irish Countrywomen's Association (ICA) staff should follow this policy when commissioning any external data processing services.

2. Policy statement

2. The ICA Data Protection Policy commits ICA to processing personal data in accordance with the eight principles of the Data Protection Act 1998 (the Act). Subsequence amendments and any enable legislation including General Data Protection Regulation (GDPR)

As a 'Data Controller', we will process personal data under the legal basis of lawfulness of processing of GDPR (Art. 6), except where the Act enables processing (for example, to comply with a court request).

3. External data processing services commissioned by ICA must comply fully with our terms and conditions regarding data security and will be regularly monitored to ensure compliance with the relevant law.

3. Privacy Impact Assessments

A Privacy Impact Assessment (PIA) must always be carried out where there is any new or modified processing of personal data on behalf of the ICA. Please refer to the ICA Data Protection Policy for guidance regarding PIAs.

4. Tendering and procuring of external processing services

Staff who are involved with procurement and tendering of goods and services which may involve the processing of personal data for any purpose including, but not limited to, membership and fundraising activities.

5. Data Processors

'Data Processors' are external agencies or persons commissioned by, or acting on behalf of, a 'Data Controller' (the ICA is the Data Controller in this instance).

A typical Data Processor would be an agency or consultant commissioned by ICA. Subcontractors commissioned by the contractor are also Data Processors according to the Act.

The ICA does not consent to the Supplier appointing any third-party processor of Personal Data under the Data Processing Agreement without its prior written consent. If the ICA has consented to the

Supplier appointing a third-party processor of Personal Data, the Supplier confirms that it has the same Data Processing Agreement as written agreement with their third-party processor. As between the ICA and the Supplier, the Supplier shall remain fully liable for all acts or omissions of any third-party processor.

The ICA must ensure any sub-contracting is carried out with its full knowledge and agreement. The ICA must have sight of, and agree to the suitability of, any contract between the contractor and sub-contractor with regards to data protection and data security.

Where external processing of a broad and deep personal dataset is to be commissioned, then the Data Protection Commissioner must be consulted first.

If any directorate is planning such an exercise, they must first contact the CEO.

6. Data transfers between the ICA and Data Processors

Electronic transfers:

Electronic transfers of personal data from and to the ICA and between Data Processors must be securely encrypted. Integrity of electronic methods of data transfer between Data Processors, or between a Data Processor and ICA, must be agreed to by the CEO at the beginning of a contract or when and as changes in procedure or contract are made. The CEO must be informed immediately by the Data Processor of any such changes.

The ICA must use a secure server for the majority of data transfers (personal or anonymous). Wherever possible, staff should use this facility for external transfers of personal data with contractors and Data Processors. The CEO should be contacted if this instance is to arise.

Emails between the ICA and Data Processors, which contain personal data should only be sent in exceptional circumstances and must be encrypted. If personal data is received without encryption, you must inform your line manager/CEO immediately.

The CEO must be consulted before any new data transfer agreements and procedures are implemented at ICA.

Any breaches of data security or data loss must be reported to the CEO immediately. Please read the guidance on ICA Personal Data Breach Notification Policy.

External transfers of personal data in hardcopy have been the cause of many data loss incidents within the sector. To mitigate against such events occurring at the ICA, hardcopy transfers must only be carried out where absolutely necessary and only then using the strictest and most secure methods available.

Points to consider when transferring personal data in hardcopy:

• Always consider whether personal identification data needs to be transferred in this way at all.

• Where it is practical, consider anonymising the personal identification data before transfer.

• If possible, separate personal identification data from the rest of the data and send each part separately.

17. Where hardcopy transfers are necessary, the procedure must be validated and agreed by the CEO.

The CEO must be informed of any new or ad hoc transfers of personal data into, or externally from, the ICA.