Northern Ireland Housing Executive Retirement Association

Data Protection Policy & Handling Instructions

Version 0.1 1st August 2023
Version 0.2 10th September 2023
Version 0.3 3rd October 2023

Introduction

The General Data Protection Regulations (GDPR) are now in force through the Data Protection Act (2018). These introduced some additional requirements for the use of personal information. As we hold personal data about our members and other individuals for a variety of business purposes we must comply with the law.

This policy document sets out how we comply with the regulations, seeking to protect personal data and ensure that all members accessing personal data understand the rules governing the use of personal data. In particular, this policy requires that the Chair be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Breaches of the regulations can attract a fine of up to the equivalent of 20 million Euro (or 4% of global turnover) however considering the quantity and type of information held this level of sanction would be very unlikely.

This document also details what information is collected and best practice as to how this information must be handled.

Scope

This policy applies to all members of The Association who have access to personal information in their voluntary role. They must be familiar with this policy and comply with its requirements.

Any new or modified policy will be circulated to members before being adopted.

Definitions

GDPR has introduced new requirements and amended existing data protection legislation. Full details of these are to be found on the UK Information Commissioner's Office website www.ico.org.uk For the purpose of this document the following definitions will be used.

Personal Data

Any information that relates to an individual, where the individual can be identified directly or indirectly from the information. This would include information relating to volunteers, current and former members, trade suppliers and other third parties that we deal with.

Sensitive Personal Data

Some personal data is more sensitive and requires a higher level of protection. This includes

- race
- ethnic origin
- political opinion
- religious or philosophical beliefs
- trade union membership

- genetic data
- biometric data (where used for identification purposes)
- health data
- sex life
- sexual orientation
- criminal convictions

The Association does not, and will not, hold such sensitive personal data.

Responsibilities

All members who access personal information must comply with this policy, however the role of Chair carries with it additional responsibilities.

- keeping the members updated about data protection responsibilities, risks and issues
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from members and others
- Responding to individuals such as subject access requests.

Mandatory Requirements

The Association's aim is to ensure that it complies with both the law and best practice, it must:

- Respect the rights of the individual
- Be open and honest when collecting information
- Notify the Information Commissioner voluntarily where appropriate
- Ensure all members who handle information are trained

Data Protection principles

Fair and lawful processing

Personal data must be processed fairly and lawfully in accordance with the individual's rights. No data may be processed or stored without a legal basis being established. This must be completed in consultation with the Chair and will be detailed in the associated Privacy Notice.

The processing of all data must be:

- In our legitimate interests and not unduly prejudice the individual's privacy. Where Legitimate Interest is claimed as a basis for processing this must be backed by a Legitimate Interests Assessment approved by the Chair.
- Where it is necessary to gain consent, this must be clear, specific and not a default option or pre ticked box.

Purpose Limitation

We must always be clear in our Privacy Notice about why we are processing information and undertake not to use this information for any other purpose

Data Minimisation

We must ensure that we only collect personal data that is necessary to deliver the stated service and must not hold more than is needed for that purpose.

Accuracy

We must take all reasonable steps to ensure that personal data is accurate. If it is discovered that personal data is incorrect or misleading reasonable steps must be taken to correct or erase it as soon as possible.

Storage Limitation

We must only hold personal information for as long as it is required and no longer than the period stated in the Privacy Notice.

Integrity and confidentiality (security)

Everyone must follow The Association's guidelines on securing personal information in order to protect the information's confidentiality and integrity.

Accountability principle

The Association is responsible for what we do with personal information and it is important that all members follow this security policy, along with any other guidance issued by The Association. This will protect individual's personal information, you and The Association.

Lawful basis for processing

No personal information can be processed without a valid lawful basis. The ICO details six lawful bases for processing and the most appropriate must be determined in discussion with the Data Protection Officer (DPO) before processing. This choice is important as it also impacts on the subject's rights. Further information is available on the ICO website and the lawful basis for processing must be detailed in the Privacy Notice.

Privacy notices

The privacy Notice is a key element in informing people as to what information is being processed or stored. This must be written in plain English. All personal information held must be covered by a privacy notice that covers the following:

- What information is being collected
- Who is collecting it
- How it is collected
- Why it is being collected
- How it will be used
- Who it will be shared with

- How to correct information
- Identity and contact details of any data controllers
- Details of transfer to third countries and safeguards
- Retention period

Individual Rights

The GDPR has a series of rights associated, these are detailed on the ICO website. All of these rights need to be responded to within one month, not all will apply, the full details of the request should be included in this response. It is also important that the individual is identified as that person and we only release personal data to the correct person, preferably to contact details previously provided. GDPR provides the following rights for individuals:

The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. This information must be provided at the time information is being collected.

We must provide individuals with information including; our purposes for processing their personal data, our retention periods for that personal data and who it will be shared with. This will be specified in the Privacy Notice.

Remember, getting the right to be informed correct will help compliance with other aspects of the GDPR and will build trust with people.

The right of accessing

Individuals have a right to access their personal data, known as a Subject Access. If a subject access request is received, either verbally or in writing, The Association has 1 month to respond.

The right to reactivation

Individuals have a right to have inaccurate personal data rectified> As with a subject access request this can be made verbally or in writing. This could be implemented as standard using a “change details request”.

The right to erasure

Individuals have a right to have personal data erased, also known as “the right to be forgotten”. This request can be verbal or in writing and must be responded to within one month.

This right is not, however, absolute and only applies in certain circumstances. For example we may remove the contact details for a member after their membership expires however we would not remove their name or membership status as that forms part of The Association's historical records. We would also have to keep details of any financial information for a period.

The right to restrict processing

Individuals have the right to restrict processing of their personal data in certain circumstances. This means that an individual can limit the way that The Association uses their data. This is an alternative to requesting erasure of the data but is a complex requirement and must be discussed with the Chair.

The right to data portability

The right to data portability gives individuals the right to receive personal data they have provided to The Association in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller. Whilst it is unlikely that such a request would be made it remains a right that could be exercised.

The right to object

The right to object to the processing of their personal data effectively allows individuals to ask The Association to stop processing their personal data. This is not absolute and each case must be discussed with the Chair.

Automated decision making and profiling

This is any form of automated processing of personal data that makes a decision that affects a person, for example to judge suitability for a loan. The Association does not use such techniques and therefore should never be affected by this.

Children

Children need particular protection when their personal data is being collected or processed as they may be less aware of the risks involved. Membership of The Association is restricted to retirees and therefore personal data of children will never be collected or processed.

Reporting breaches

The Information Commissioner defines a personal data breach as follows:

A 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. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

When a personal data breach has occurred the likelihood and severity of the resulting risk to people's rights and freedoms must be established. If it is likely that there will be a risk the ICO must be notified; if it’s unlikely it does not need to be reported. If it is decided not to report to the ICO this should be documented as the decision may have to be justified.

GDPR introduces a duty on all organisations to report certain types of personal data breach within 72 hours, where feasible, of becoming aware of the breach. If the breach is

likely to result in a high risk of adversity affecting individuals' rights and freedoms they must be informed without undue delay.

All breaches will be reported through the Chair who will determine if it is reportable. Additionally the Chair will co-ordinate all remedial responses and maintain a register of any personal data breaches regardless of whether The Association was required to notify the ICO. Breaches can be reported via the ICO website.

Training

All members who handle personal information will receive training on this policy, further training will be provided at least every two years or whenever there is a substantial change in the law, our policies or procedures.

The Association will appoint a Data Protection Officer (DPO) who will not have any access to member's personal data. The DPO will arrange training as required and this may be in conjunction with the NIHE.

Training will cover:

- The law relating to data protection
- Our data protection policies and procedures
- Security awareness
- Security best practice

Handling information

Everyone who comes into contact with The Association's information and data must make sure they understand its content, know how to handle it and know how to destroy it.

User access

Users must only be given the minimum of access to personal information to meet their role, once that role has finished the access should be removed and they should confirm that any information has been destroyed or returned.

Handling Instructions

This section details what information The Association uses, how it is held and who holds it.

The information held is the Member's name, address and date of leaving only, this does not pose any risk to the Member's freedoms or legal rights. The information is used as follows:

Communications with members

All communications should be via information extracted from The Association's database for a specific purpose. This ensures that only members who have agreed to receive communications are contacted and that we use the most up to date information. This information is maintained by the Chair and appointed officers. This is important as:

- it reduces the need for details to be held in personal email systems
- it ensures we are using the most up to date information
- we are only contacting members who wish to be contacted
- it will simplify any request for information held

This information must not be extracted from The Association's database for any other use.

This information is only accessible to the Chair and any appointed officers with access being controlled by the Chair.

Should members be contacted using personal e-mail (for example replying to a query from a member) this email should be deleted once the issue or request has been dealt with. Good email hygiene helps to ensure that we can confidently respond to access requests knowing that we have nothing held on e-mail.

It is also recognised that The Association was established as a social provider and through membership of The Association there will be many friendships that are on a personal level and outside the scope of data protection

Finance Records

All financial records are maintained by the responsible member. These records are kept in both paper and electronic formats. The only personal information contained in these records is the member's name, or in the case of donations or payments the donor or recipient name.

Paper records are held securely in a locked case under the responsible person's control and form the "working copy" of the accounts.

The electronic version is created from the paper working copy, this is held as an encrypted, password Excel file. This file is normally only shared with the account examiners and a summary paper copy is produced for members inspection at the AGM, this copy does not contain member's personal information.

Electronic records are kept for five years before being deleted securely.

Attendance records

The attendance records are normally held as part of the financial records of The Association. The paper copies are part of the working copy, the same form being used to record payments and expenditure during a meeting.

The paper copies are maintained until the end of the next membership year and then destroyed securely. The attendance information is added to the electronic record and kept for the same five years. Names of visitors are not recorded electronically and are deleted as part of the paper financial records.