The NatWest Group
Pensioners Benevolent Fund

Registered Charity No. 277974

Data Protection and Data Security Policy

Last Reviewed
October 2023

Contents

The NatWest Group Pensioners Benevolent Fund

Data Protection and Data Security Policy

Introduction

The NatWest Group Pensioners Benevolent Fund ("the Fund") holds personal data about its applicants. The Fund needs to hold information about its applicants to support its core function of processing and approving or declining applications for financial assistance. Data may also be held on other individuals, such as enquirers to the Fund, ahead of them submitting an application to the trustees.

The General Data Protection Regulations 2018 (GDPR) places responsibilities and obligations on organisations which process data about living individuals. It also gives legal rights to individuals in respect of personal data held about them by others.

The Fund is required to have policies and procedures in place to ensure compliance with its obligations under the GDPR that extend across its trustees and the activities of the Fund.

Purpose

This document defines the Fund's policy on data protection and data security and is based on the following principles:

- The Fund will comply with all relevant legislation, particularly the GDPR, and base its policies and practices on compliance with the data protection principles contained therein.
- Ensuring compliance is a corporate responsibility of the Fund requiring the active involvement of, and appreciation by, all trustees.
- The Fund will strive to ensure best practice with regard to data protection and data security processes and procedures.
- The Fund trustees will strive to remain compliant with the legislation and the Fund's requirements in respect of data security.

Scope

This policy applies to:

- All trustees of the Fund
- Any staff employed by the Fund
- Any third party individuals with any degree of access and/or use of personal data held by the Fund.

It will be reviewed at least annually to ensure its continued appropriateness and approved at a meeting of the Trustees prior to any changes being implemented.

Definitions

The following definitions apply to this policy:

- GDPR: The General Data Protection Regulations, 2018.
- Data security breach: Any occurrence of any unauthorised or unlawful processing of personal data held by the Fund, or the accidental loss, destruction of or damage to any such personal data.
- Data subject: A living individual who is the subject of personal data.
- Data controller: A person or organisation which controls the purposes and manner in which data are processed. The Fund is a data controller, and the point of contact is the trustee with oversight of data protection.
- Data: All information in electronic or physical format.
- The Information Commissioner (ICO): The supervisory authority, reporting directly to Parliament, that enforces and oversees adherence to GDPR, and other information related legislation. The ICO maintains a public register of data controllers.
- Personal data: Data which relate to a living and identifiable individual, including computerised data and some manual data (i.e. paper-based records, microfiche, etc.). Processing: An action of any sort taken in regards personal data during the lifecycle of that personal data. This will include but is not limited to, obtaining, storing, adapting, transferring, transmitting, disposal and destruction.
- Sensitive personal data: The GDPR recognises that certain types of personal data should be treated with particular regard. Such data include racial or ethnic origin; political opinions; religious beliefs; membership of a trade union; physical or mental health or condition; sexual life; and criminal offences.
- Subject Access Request (SAR): The means by which any individual exercises the right, pursuant to section 7 of the DPA any individual to see a copy of the information an organisation holds about them. A SAR can include the following elements:
    - a request to be told whether any personal data is being processed;
    - a request to be given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
    - a request to be given a copy of the information comprising the data; and
    - a request to be given details of the source of the data (where this is available).

Aims

The aims of this Data Protection and Data Security Policy are to:

- Set out the obligations of the Fund with regard to data protection and data security.
- Establish the guiding principles for the Fund's actions in this area.
- Provide a policy framework to ensure local compliance with GDPR and the Fund's requirements in respect of data security.

Policy statements Notification

The Fund will comply with the notification obligations placed upon it by the GDPR and associated regulations; specifically renewing notification with the ICO yearly and ensuring that the notification is current and accurate.

Personal data held by the Fund

Data are collected from applicants at various stages of the application processing procedure. Examples include, but are not restricted to:

- personal details on application forms
- health related data such as Occupational Therapist's report
- local authority DLA/ PIP approval letters
- evidence of NWG pension (P60 or pension advice slip)
- quotations, invoices and receipts.

All applicants have a responsibility to ensure that any information that they provide to the Fund in connection with their application is accurate and up to date.

Data Protection Principles

The Fund is committed to processing data in accordance with its responsibilities under the GDPR. Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
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;
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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
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."

1. General provisions

a. This policy applies to all personal data processed by the Fund.
b. This policy shall be reviewed at least annually.
c. The Fund is registered with the Information Commissioner's Office as a data controller that processes personal data.

2. Lawful, fair and transparent processing

a. Individuals have the right to access their personal data and any such requests made to the Fund shall be dealt with in a timely manner.

3. Lawful purposes

a. All data processed by the Fund must be done on the basis of consent.
b. Evidence of opt-in consent shall be kept with the personal data. A data protection notice is included on the Fund's application form which sets out the data which are collected, the

uses to which they will be put, and seeks consent for their processing

c. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Fund's systems.

4. Data minimisation

a. The Fund shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

5. Accuracy

a. The Fund shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

6. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Fund shall put in place an archiving/ data retention policy for each area in which personal data is processed and review this process annually.
b. The archiving/ data retention policy shall consider what data should/must be retained and for how long.

7. Security

a. The Fund shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to those trustees who need access and appropriate security should be in place to avoid unauthorised sharing of information. Such security measures could include: restricting access to the data to the minimum number of persons possible; ensuring that all digital personal data is password protected wherever it may reside; ensuring that any personal data are not left 'in the open' either in paper form, or on a screen in digital form; ensuring that access to the area in which the personal data is stored is restricted to only those persons who need to be there;, minimising the need for transfer of the data, if transfer is required.
c. Requirements for trustees' use of personal devices:

    i. An appropriate password/passcode must be set for all accounts on each device.
    ii. A password protected screen saver or screen lock must be used.
    iii. All devices must be set to lock automatically after a set period (5 minutes maximum) and require a password to unlock after this time.
    iv. The device must run the latest version of the operating system and be updated with software updates/security patches in a timely fashion.
    v. Appropriate measures should be taken to protect devices from viruses, malware, ransomware, Trojans, worms and malicious code.
    vi. Any device used for the Fund's purposes should only be used by an authorised person. If family or friends are to use the device then it must be managed in such a way that others do not have access to the Fund's information.

d. Guidelines for trustees' use of personal devices:

    i. Do not undermine the security of the device for example by Jail Breaking an iPhone.
    ii. Minimise the amount of sensitive/confidential data stored on the device.

iii. If a device needs to be repaired, ensure that the company you use has an agreement in place which guarantees the security of any data on the device.
iv. Do not leave devices unattended where there is a risk of theft.
v. Be aware of people around you when entering passwords or accessing Fund information on the device.

e. Where it is legitimate to share personal data with external organisations, the following hierarchy of actions should be adhered to:

i. Data should be uploaded via a secure portal wherever possible; most organisations using this method publish details of security systems on their websites.
ii. Where there is no secure portal, data should be transmitted electronically (for example, as files, databases, PDF files, images) over secure networks. These files should be encrypted and, if so, then email is acceptable for such transmission.
iii. If it is unavoidable to share paper copies of sensitive data, they should be mailed in securely sealed envelopes and sent by courier or registered post. An individual's personal data in the form of, for example, application approval letters or receipts, may be sent in sealed envelopes using normal postal systems.

8. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Fund shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

Data Subject Access Requests (SAR)

Persons about whom the Fund holds data (data subjects) may make a Subject Access Request (SAR) to see those data, and to receive or view copies of those data in permanent intelligible form (print-outs or photocopies).

The Fund's trustee with oversight of data protection will co-ordinate the request centrally. Requests can be made verbally or in writing. Persons making a SAR will also be required to confirm their identity. The GDPR provide that the Fund must respond to a formal request within one month.

Data storage, retention and disposal

Data at the Fund are retained and disposed of according to need. The overarching principle is that data should only be retained and stored for as long as such data have a legitimate purpose, and thereafter they should be disposed of securely. The Fund's Data Retention Policy holds a Data Retention Schedule which specifies the nature of the data retained and the retention period.

At the end of the retention period, data should be disposed of and/or destroyed. Manual files should be shredded and disposed of in designated confidential waste sacks if appropriate. Electronic data should be deleted from central systems by the individual responsible for the data.

References

This policy is supported by the following documents:

- Data Retention Policy.