

## The Vaillant Group Pension Scheme (the Scheme)

### Data protection policy

This policy sets out the Trustees' approach to complying with its obligations under the data protection laws which apply from 25 May 2018.

The Trustees recognise that it is important to keep personal information about the Scheme's beneficiaries secure and to process this information in accordance with the data protection laws. This policy has been adopted to explain how the Trustees will comply with these laws.

#### **Controller**

The Trustees recognise that they are a controller for the purpose of the data protection laws. As such, the Trustees are responsible for compliance with the data protection laws and for overseeing those who process data on the Trustees' behalf. Those who process data on the Trustees' behalf are known as their processors.

The Trustees understand that, for some purposes, some of their professional advisers, including the Scheme actuary, legal adviser and auditors, will also be controllers.

#### **Processors**

The Trustees' processors include the Scheme administrators and other service providers who are not themselves controllers.

The Trustees will ensure that their processors have provided suitable guarantees about their compliance with the data protection laws and have entered into an agreement with the Trustees that meets the requirements of the data protection laws.

#### **Overriding principles when acting as controller**

The Trustees will ensure that personal information is:

- processed in a lawful, fair and transparent manner;
- collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes;
- limited to what is necessary;
- accurate and kept up to date;
- kept no longer than necessary; and
- kept secure and protected against unauthorised or unlawful use and against loss, destruction or damage by using technical or organisational measures.

The Trustees will also ensure that data subjects' rights are honoured where appropriate.

#### **Basis for processing personal information**

The Trustees will usually process personal information because it is necessary for compliance with their legal obligations and/or because they have a legitimate interest in doing so. This is because the data is required for the administration of the Scheme. In particular, it is required to calculate and pay benefits, to advise members about their options and to deal with any queries that they have. It is also needed to ensure that the Scheme operates efficiently and provides accurate information to members.

Sometimes, the Trustees may rely on other grounds for processing personal information, such as it being necessary to comply with our obligations.

Occasionally, information may be processed on the basis that the members have consented to this, for example where information relates to 'special category data', such as health data.

In the case of 'special category data', processing may also take place without consent where this is permitted by the data protection laws. For example, such processing may take place where processing is necessary for the purpose of exercising obligations or rights under laws in connection with employment, social security or social protection, for the purpose of assessing working capacity or for medical diagnosis.

The processing of information relating to criminal convictions (if these relate to money owed to the Scheme's employers) may also take place where the member has consented to this or where it is necessary for the purpose of the establishment or exercise of a legal claim.

Where consent is relied upon, it must be explicitly given and not implied. Members will be told about their right to withdraw their consent at any time. As consent must be specific, the Trustees will generally take professional advice before seeking consent from members, to ensure that the consent is properly given. The Trustees will also generally take professional advice before processing 'special category data' without consent or before processing information relating to criminal convictions.

Information about this will be set out in the Trustees' privacy notice.

The policies set out below apply in all cases, including in relation to the case of 'special category data' and information relating to criminal convictions.

## Privacy notice

The Trustees will issue a summary of the privacy notice to all existing members and to individuals in receipt of survivor's benefits from the Scheme. The summary privacy notice will set out what the new Data Protection regulations mean for individuals, what the Scheme will and will not do with personal data, what rights the individual has in relation to the data held in relation to them, and what happens in the event of a data breach. The summary privacy notice will provide individuals with a link to the Scheme website from where they can access the full privacy notice and it will further confirm that individuals can request a printed version of both the full Data Protection Policy and Privacy Notice if they prefer.

The full privacy notice will set out:

- the Trustees' contact details;
- the purposes of the processing and the legal basis for this;
- the categories of data held;
- the recipients or categories of recipients of the data;
- information about transferring data outside of the UK or the European Economic Area (EEA) and of the safeguards in place;
- details of the period for which data will be retained;
- the existence of the right to access data and of the right to have it rectified or erased;
- the right to withdraw consent (where consent is being relied upon);
- the right to complain to the ICO; and
- details of where the data originates from if collected from a third party.

The Trustees will review the privacy notice on an annual basis and will review it before undertaking any new processing activity (like a Pensions Increase Exchange or Trivial Commutation Exercise). If necessary, an updated notice, or other form of communication, will be issued before any new processing activity is carried out.

## Retention of personal information

The Trustees recognise that personal information should only be retained for so long as necessary.

Where a person retires on a pension under the Scheme, the Trustees believe that it is necessary to retain their personal information until the member's death. If a pension death benefit becomes payable, the information will be retained until that pension ceases. Once there is no further liability, the information will be kept for as long as the Trustees believe there is a lawful reason to do so in case any future claims are made. This will be for the entire life of the Scheme and for a period of 6 years after all members' entitlements have been extinguished.

Where a member transfers out of the Scheme or takes all benefits as a cash sum, the member's personal information will be kept for as long as the Trustees believe there is a lawful reason to do so in case any future claims are made. This will be for the entire life of the Scheme and for a period of 6 years after all members' entitlements have been extinguished.

The Trustees believe that retaining personal information for this length of time is in line with their obligations, their legitimate interests and the interests of the Scheme as a whole and is also in the interests of the people concerned. This is because it is important to be able to demonstrate that benefits have been paid correctly and that the Scheme has discharged its liabilities and to be able to deal with any queries raised about this in the future.

## Right to access personal information

The Trustees will seek to comply with access requests and to provide the appropriate data within one month of a request being made. Where this isn't possible, the member will be kept informed. The Trustees will take professional advice about how to comply with any request, to ensure that appropriate information is provided. Usually there will be no charge for providing the information.

In the unlikely event of manifestly unfounded or repetitive requests, the Trustees may decide not to provide information. However professional advice will be taken in those circumstances.

## Right to rectify personal information

It is important that personal information is accurate. The Trustees shall seek to verify data at appropriate times. The Trustees shall also ensure that members are regularly reminded of the need to update their contact details and any expression of wish forms.

## Right to have personal information deleted and to object to processing

The Trustees recognise that the right to have personal data deleted (the right to be forgotten) is not an absolute right and is subject to any overriding interest that the Trustees may have which justifies the retention and processing of the information. As such, during the period referred to in the section '**Retention of personal information**' opposite, the Trustees are unlikely to be required to honour a request for data to be deleted.

Similarly, members have the right to object to the Trustees' legitimate interest in processing data. If they do this during the period referred to in the section '**Retention of personal information**' above, the Trustees are likely to conclude that they have an overriding interest which justifies the retention and processing of the information.

## Records of processing activities

The Trustees will maintain a written record of their processing activities as controller. This will set out:

- names and contact details and those of any joint controller;
- the purpose of the processing;
- the categories of data subjects and the categories of personal data;
- the categories of recipients to whom data has been or will be disclosed;
- details about transfers of data outside the EEA, including the name of the recipient country, and of the safeguards in place;
- the time limit for retention of the data;
- a general description of the technical and organisational security measures implemented; and
- information relating to the conditions under which special category data and information relating to criminal convictions is processed.

The Trustees' processors must maintain similar records.

## Measures to ensure data security

The Trustees must take appropriate technical and organisational measures to ensure personal information is kept secure and protected against unauthorised or unlawful use and against loss, destruction or damage.

The Trustees' policy is that the following measures should usually be taken:

- all paper-based documentation containing personal information should be disposed of in a confidential manner, e.g. using confidential shredding bins;
- those working with personal information should maintain a clear desk and clear screen when they leave their workstation;
- all storage facilities which contain personal information should be locked when unattended or be within locked premises;
- personal data should be kept secure whenever it is outside of the premises, e.g. on a password protected device;
- access to personal data should be limited to access for legitimate business purposes only;
- where possible, personal data should be transferred by encrypted means; and
- where possible, personal information should be anonymised before it is used, especially where it is being shared amongst the Trustees or with third parties.

The Trustees will seek to ensure that the Trustees' processors comply with its policies or otherwise take measures which are acceptable to the Trustees.

The Trustees will monitor their processors by a combination of:

- carrying out due diligence prior to appointment (for any new processors);
- contractual arrangements which include the mandatory contractual provisions;
- periodic assessments; and
- audit requirements.

## Transfers of data outside the EEA

The Trustees will seek to ensure that data is not transferred outside the EEA without appropriate safeguards being in place. Where the data is not transferred to an EU Commission approved country, appropriate contractual safeguards will be required.

Professional advice will be taken if it is proposed that personal information be transferred outside the EEA directly by the Trustees. Transfers outside the EEA may be made by the Trustees' processors where this is permitted by their prior agreement with the Trustees.

## Dealing with breaches of the data protection laws

The Trustees recognise that breaches of the data protection laws can have serious consequences and must be dealt with quickly.

As such, the Trustees have delegated authority to deal with data breaches to any two members of the Trustee board.

Professional advice will be sought about how to deal with the breach and whether the Information Commissioner's Office (ICO) and the members concerned need to be notified.

Notification to the ICO is required without delay (and in any event within 72 hours) unless the breach is unlikely to result in a risk to the member concerned. Members must be notified without undue delay where the breach causes a high risk to them.

Those who process data on behalf of the Trustees are required to notify them of any breach without undue delay after becoming aware of it.

## Data protection officer

The Trustees have not designated a Scheme specific data protection officer, however Vaillant Group will be appointing a data protection officer who will oversee all Data Protection requirements across the business. The Scheme specific data protection responsibilities will be managed locally by the Vaillant Group Pension Scheme Pensions Manager and this will ensure the Company (in its capacity as a major supplier of data heavy administration services to the Trustees) is at all times aware of its obligations and duties under Data Protection, and discharging its responsibilities effectively.

Contact details for Data Protection matters are as follows;

Steve Tickner  
Pensions Manager  
Vaillant Group UK Ltd  
Nottingham Road  
Belper  
Derbyshire  
DE56 1JT

Phone: +44 (0)1773 596250

Email: [Steve.Tickner@vaillant-group.com](mailto:Steve.Tickner@vaillant-group.com)

### **Data protection impact assessments**

If the Trustees believe that a new form of processing will carry a high risk, for example if it uses new technologies, an impact assessment may be carried out.

However, in many cases the Trustees expect that their processors will have carried out assessments in those circumstances as to the level of risk involved.

### **Board supervision**

Reflecting the importance of their data protection obligations, the Trustees will ensure that data protection is reviewed on at least an annual basis and that this incorporates a review of the data retention policy in order to be satisfied that there is an ongoing legitimate reason to continue holding data.