# DATA PROTECTION POLICY

# THE AQA PENSION SCHEME

## 1. ABOUT THIS POLICY

1.1 The purpose of this data protection policy (the "**Policy**") is to explain, in broad terms, how the Trustees ("**we**" or "**the Trustees**") of the AQA Pension Scheme ("**the Scheme**") will comply with data protection laws, including the European General Data Protection Regulation ("**GDPR**") as it applies to the laws of England and Wales (**"the UK GDPR"**) and the Data Protection Act 2018.

1.2 Under data protection laws, the Trustees are the data controllers for the purposes of the Scheme. As such they have legal responsibilities as data controller.

1.3 Data subjects have rights under data protection laws as to how their personal data is handled. During the course of our activities the Trustees will collect, store and process personal data about data subjects who include Scheme members, their dependants, beneficiaries, service providers' employees and other third parties. The Trustees recognise the need to treat personal data in an appropriate and lawful manner in accordance with data protection laws (including as to how the information is processed).

1.4 This Policy is subject to review from time to time, normally annually, to ensure compliance and best practice. Should there be any change, or expected change, in data protection laws this Policy will be reviewed. Where appropriate the Trustees will obtain professional advice. This Policy may be amended at any time by agreement of the Trustees, following which a replacement policy will be issued.

## 2. TERMS USED IN THIS POLICY

2.1 In this Policy, we use the following terminology:

**Data subjects** include all living individuals about whom the Trustees hold personal data. A data subject need not be a national or resident of the United Kingdom. All data subjects (irrespective of nationality or residency) have legal rights in relation to their personal data. In the context of our operations, Scheme members, their dependants and beneficiaries will generally be data subjects.

**Personal data** means any information relating to a living individual who can be identified from that information (or from that information and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion. The scope of the definition of personal data is very wide.

**Data controllers** are the organisations which determine the purposes for which, and the manner in which, any personal data is processed. Generally the Trustees are the data controller of all personal data the Trustees hold in connection with the Scheme.

**Data processors** include any company or other person which processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition. It will include any administrators and/or suppliers that handle personal data on our behalf.

**Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

**Sensitive personal data** means information about a person's:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- trade union membership;
- physical or mental health or condition or sexual life;
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Sensitive personal data can only be processed under strict conditions, and will often require the express consent of the person concerned. To the extent that that a privacy impact assessment needs to be carried out before sensitive personal data can be processed, the Trustees will take appropriate advice and discuss all proposed activities which may require the completion of such an assessment.

## 3. THE DATA PROTECTION PRINCIPLES

3.1 Where the Trustees themselves process personal data, the Trustees will comply with the following principles of good practice. The Trustees will ensure that personal data is:

(a) processed lawfully, fairly and in a transparent manner;

(b) processed for limited purposes and in an appropriate way;

(c) adequate, relevant and not excessive for the purpose;

(d) accurate;

(e) not kept longer than necessary for the purpose;

(f) processed in line with data subjects' rights;

(g) secure; and

(h) not transferred to people or organisations situated in countries without adequate protection of data subject's rights and freedoms.

3.2 The remainder of this Policy describes our requirements in relation to these principles.

3.3 The Trustee must implement appropriate technical and organisational measures in an effective manner to ensure compliance with these principles, including having adequate resources and controls in place to ensure and to document UK GDPR compliance including:

(a) implementing privacy by design when Processing Personal Data and completing a privacy impact assessment where Processing presents a high risk to rights and freedoms of Data Subjects;

(b) integrating data protection into internal documents including this Data Protection Policy;

(c) regular training on the UK GDPR, this Data Protection Policy and data protection matters, and keeping a record of this training;

(d) keeping full and accurate records of all Processing activities; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

## 4. LAWFUL, FAIR AND TRANSPARENT PROCESSING

4.1 This Policy seeks to ensure that the processing of personal data is done fairly and without adversely affecting the rights of the data subject.

4.2 Data subjects will be notified by the Trustees that personal data is being processed by them, the legal basis for processing and the purpose for processing. Whilst, in practice, these matters may be obvious from their context, the Trustees are nevertheless required under the UK GDPR to explain these matters (as well as other matters) to the data subjects by sending them a data privacy notice. A copy of the data privacy notice which the Trustees have sent to Scheme members is attached in the Appendix to this Policy for information. In the event that the Trustees undertake new or different processing they will consider whether the data privacy notice has to be updated and resent to the Scheme members. For personal data to be processed fairly and lawfully, certain conditions have to be met. The conditions which are likely to be relevant to our activities are:

(a) **Legitimate interests grounds** – This requires that the processing is necessary for the legitimate interests of the Trustees (for example they are responsible for administering the Scheme and delivering the benefits and so it is in their legitimate interests to process the personal data) or the legitimate interests of the third party to whom it is disclosed (for example the Scheme actuary who requires the personal data to undertake the Scheme valuation). The Trustees rely upon the "legitimate interests" ground as the legal basis for processing members' personal data. The legitimate interests are the administration of the Scheme in order to pay each member's benefits. However, such legitimate interests may be overridden by the interests or fundamental rights and freedoms of the data subject.

(b) **Explicit consent from the data subject** – Where the Trustees are processing sensitive personal data, they will comply with the explicit consent requirement and obtain this from the data subject before processing the sensitive personal data.

(c) **Obligations and rights in the field of employment and social security law** – This condition may be relied upon where the Trustees are processing sensitive personal data and it is not appropriate to seek explicit consent from the data subject.

## 5. PROCESSING FOR LIMITED PURPOSES ONLY

5.1 Personal data will only be processed by the Trustees for the specific purposes identified when the data was first collected or for any other purposes specifically permitted by applicable data protection laws. This means that personal data should not be collected for one purpose and then used for another. If it is necessary to change the purpose for which the data is processed, the Trustees will inform the data subject about the new purpose before processing occurs. In case of any doubt as to whether any particular proposed activity is permitted the Trustees will take appropriate advice.

5.2 Personal data about Scheme members. Personal data about Scheme members may be processed (including by disclosing the personal data to third parties) to enable the Trustees to carry out obligations related to the Scheme's administration, including the calculation and delivery of benefits and related entitlements. The Trustees may also disclose personal data of Scheme members to third parties. For example, in the event that the Trustees wish to enter a buy-out/buy-in of any of the benefits under the Scheme, the Trustees may disclose such personal data to the prospective counterparty to such a transaction. The Trustees may also disclose such personal data if they are under a duty to disclose or share such personal data in order to comply with any legal obligation. Personal data of Scheme members or their dependants or beneficiaries may be sensitive personal data for which explicit consent of the data subject is required before the data can be processed.

5.3 Service provider data. The Trustees also process data about the Scheme's current and potential service providers (such as pensions administration service providers, tracing agencies, scheme actuary, lawyers, accountants and similar advisors). Any personal data the Trustees hold will generally be about individual representatives of our service providers and typically will include contact and other biographical details. The Trustees may process this personal data for administrative and account management purposes. The Trustees will not process any sensitive personal data about their suppliers.

## 6. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

6.1 Personal data will only be collected to the extent that it is required for the specific purpose identified at the time of collection. Any personal data which is not necessary for that purpose should not be collected in the first place.

6.2 Where the Trustees are collecting personal data it is good practice to minimise the amount of data collected but there is a clear balancing act between this consideration and fulfilling and anticipating the requirements of the Scheme. The Trustees will be practical in undertaking this assessment but will always have regard to this Policy in doing so.

## 7. ACCURACY OF DATA

7.1 The Trustees will ensure that personal data will be accurate and kept up to date as far as practicable. Information which is incorrect or misleading is not accurate and steps will be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Any Trustee who becomes aware of any information that is inaccurate will inform the Chair of the Trustees.

## 8. RETENTION OF DATA

8.1 Subject to Clause 9.2 below, personal data will not be kept for longer than is necessary for the purpose for which it is held. This means that data should be destroyed or erased from our systems when it is no longer required. It is always good practice to minimise the length of time data is held, but there is a clear balancing act between this consideration and fulfilling and anticipating the requirements of the Scheme.

8.2 In general, the Trustees will keep personal data relating to Scheme members for as long as they (or their dependants or beneficiaries) have an entitlement to any form of benefit and for such further period as may be appropriate for the purposes of maintaining records of steps the Trustees have taken to comply with their obligations under the Scheme. Inevitably, this means that personal data may be retained by the Trustees for extremely long periods of time, including after entitlement to receive benefits by an individual and/or their beneficiaries has ceased. The end date for holding data in respect of a particular beneficiary is expected to be 15 years from the date on which the Scheme terminates.

## 9. PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

9.1 Data will be processed in line with data subjects' rights. Their rights include the following:

(a) the right to request access to any data held about them by us as a data controller (see below in section 14 (*Subject Access Rights*);

(b) the right to receive a copy of their personal data in a structured, commonly used and machine readable format so that they can share it with others, or to have their personal data transferred to another data controller;

(c) the right to ask to have inaccurate or incomplete data rectified or completed;

(d) the right to ask for their personal data to be erased; and

(e) the right to ask for the processing of their personal information to be restricted or stopped (for example but without limitation, where the Trustees use personal data for automated decision making purposes).

9.2 However, if a data subject asks the Trustees to erase or to stop or restrict the processing of their personal data, the Trustees may be unable to properly administer the Scheme or process any benefits for any such data subject, and if the Trustees have compelling legal grounds to continue to process such personal data, they may continue to do so.

## 10. DATA SECURITY

10.1 The Trustees will always ensure that appropriate security measures are implemented against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. The Trustees have had confirmation, which they will re-assess from time to time, from all other data controllers and data processors of data in respect of the Scheme that they have put appropriate security measures in place.

10.2 Where appropriate, personal data should be anonymised or pseudonymised. Individual Trustees themselves will not store non-anonymised personal data on their own PC drives or other personal devices or in hard copy and will not share any non-anonymised personal data by unencrypted communications media (including e-mail etc.)

## 11. PROVIDING INFORMATION TO SERVICE PROVIDERS

11.1 The Trustees regularly engage the assistance of third party service providers who will have access to personal data to provide their services, such as pensions administration service providers, tracing agencies, lawyers and accountants.

11.2 If the Trustees do transfer personal data to any service provider:

(a) the Trustees will undertake appropriate checks to make sure such processor provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Data Protection Act 2018 and the UK GDPR;

(b) the Trustees will ensure the service provider enters into a written contract which contains a contractual commitment from the service provider to this effect and the Pensions Manager and/or Secretary to the Trustees will maintain records of the written arrangements the Trustees have in place with all service providers who are permitted to process personal data; and

(c) the Trustees will undertake ongoing monitoring to ensure the service provider complies with these commitments (the extent of the monitoring will be dependent on the nature of the service provision).

## 12. TRANSFERRING PERSONAL DATA OUTSIDE THE UNITED KINGDOM: ENSURING ADEQUATE PROTECTION

12.1 Organisations that collect and otherwise process personal data inside the United Kingdom (**"UK"**) are required to do so in compliance with UK data protection laws that prohibit the transfer of personal data to parties that are located outside the UK unless adequate protections exist.

12.2 Generally the Trustees will not transfer personal data outside the UK. The Trustees may only transfer or grant access to the personal data to other parties that are located outside the UK if the recipient is located in a country which the UK Government has decided offers adequate protection (as of November 2023, these countries are countries in the European Economic Area, Andorra, Argentina, Canada, Faroe Islands, Guernsey, Japan, Jersey, the Isle of Man, Israel, New Zealand, Switzerland and Uruguay) or if that recipient agrees to enter into a standard form data transfer agreement approved by the UK Government for this purpose called the international data transfer agreement, or the EU standard contractual clauses with the UK international data transfer addendum.

12.3 Additionally, the Trustees may transfer or grant access to personal data to parties located in the United States if the recipient is part of the EU-US Data Privacy Framework. The list is available here: https://www.dataprivacyframework.gov/s/ .

12.4 The Trustees will not transfer personal data to an entity which is located in a country outside the UK unless the Trustees are satisfied that appropriate contractual or other arrangements are in place to protect the personal data as explained in section 12.2 and 12.3 above. The Trustees will take appropriate advice on any questions about transfers of personal data outside the UK.

## 13. PROVIDING INFORMATION TO OTHER THIRD PARTIES

13.1 There will be occasions when the Trustees are asked or obliged to provide personal data to third parties (who are not data processors); for example, to government agencies, tax authorities, law enforcement agencies or when required by a court order. The Trustees may also be asked to provide personal data to a prospective counterparty in the event of a proposed buy-out/buy-in of any of the benefits under the pension schemes.

13.2 When dealing with enquiries from third parties the Trustees will:

(a) check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested;

(b) suggest that the third party put their request in writing so the third party's identity and entitlement to the information may be verified;

(c) take appropriate advice in difficult situations; and

(d) where providing information to a third party, do so in accordance with the data protection principles set out in section 3 (*The Data Protection Principles*) above, including, where possible, putting an agreement in place with the third party that will detail how they will use the personal data provided to them (as well as a data transfer agreement, to the extent the third party is located outside of the UK).

## 14. SUBJECT ACCESS REQUESTS

14.1 As set out in section 9 (*Processing in line with Data Subjects' Rights*), a data subject has a right to ask for a copy of any personal data about them which the Trustees hold. A formal request from a data subject for their personal data (in writing) must be made. The information must be provided free of charge except that the Trustees may charge a reasonable fee if a request is manifestly unfounded or excessive, particularly if it is repetitive.

14.2 Any written request from a data subject in relation to his rights as listed in section 9 will be forwarded to the Pensions Manager and/or Secretary to the Trustees immediately because the Trustees are subject to strict time limits for compliance with requests of this nature and because careful judgements may need to be taken where the personal data requested might also include personal data of others.

15. **SECURITY BREACHES RELATING TO PERSONAL DATA**

15.1 Suspected breach. If any of the Trustees or the Pensions Manager and/or Secretary to the Trustees suspects that personal data has been lost, stolen, corrupted or accessed without authorisation, they will contact the Chair of the Trustees and (if it is not the Pensions Manager and/or Secretary who suspects the breach) the Pensions Manager and/or Secretary immediately and inform them of the suspected breach.

15.2 Discovered breach. If the Trustees or the Pensions Manager and/or Secretary to the Trustees discover a breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored otherwise processed ("**personal data breach**"), the following steps will be taken:

(a) if any of the Trustees or the Pensions Manager and/or Secretary to the Trustees discovers, or is informed by a third party of, the personal data breach, it must be reported immediately to the full Trustee board and (if it is not the Pensions Manager and/or Secretary who has discovered or is informed of the breach) the Pensions Manager and/or Secretary.

(b) If the Pensions Manager and/or Secretary to the Trustees discovers the personal data breach, he/she must report the personal data breach immediately to the full Trustee board;

(c) immediately upon being notified of the personal data breach the Chair of the Trustees shall assemble a team of individuals ("**Team**"). The Team must always include the Pensions Manager and/or Secretary to the Trustees and the Chair of Trustees (or failing that another Trustee appointed with the agreement of a quorum of the Trustee Board) and any other person deemed appropriate. The Chair will also promptly inform AQA;

(d) the Team shall, on behalf of the Trustees, (i) investigate the nature, cause and seriousness of the breach; and (ii) assess the risks of the breach causing damage to the data subjects. Following investigation by the Team, the Chair will report to the full Trustee board and will instruct the Pensions Manager and/or Secretary to notify the personal data breach to the Information Commissioner's Office on the Trustees' behalf as soon as possible and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to any individual's rights and freedoms in which case no such notification is necessary. Notification should be made via the Information Commissioner's website: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/;

(e) if the Team, on behalf of the Trustees, concludes after assessment of the risk to the data subjects that the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects and/or other persons, the Chair will instruct the Pensions Manager and/or Secretary to communicate the personal data breach to the data subjects on behalf of the Trustees without undue delay; and

(f) following resolution of the breach, the Chair of the Trustees (with appropriate advice if necessary), will evaluate the identification and causes of the personal data breach as well as the response and instruct the Pensions Manager and/or Secretary to amend any deficient security, procedures and policies accordingly as soon as possible**.** The Pensions Manager and/or Secretary will provide the Trustees with a report on the personal data breach including the results of the investigation, assessment of risk impact on the data subjects, response of the Information Commissioner's Office, resolution of the breach and how deficient security has been resolved.

15.3 Information to be provided to data subjects. In the event of a breach requiring data subjects to be notified, the notice will:

(a) describe in clear and plain language the nature of the personal data breach;

(b) give the name and contact details of the person data subjects can contact for more information;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken, or proposed to be taken, to deal with the personal data breach including, where appropriate, the measures taken to mitigate any possible adverse effects; and

(e) anything else that is relevant in the circumstances, including any steps which it is recommended data subjects take to protect their own personal data.

## 16. AUTOMATED DECISION MAKING

16.1 Automated decision making is when a decision is made which is based solely on automated decision making which produces legal effects or significantly affects an individual. Profiling is an example of automated decision making, as are many uses of artificial intelligence where they involve the processing of Personal Data. The UK GDPR prohibits this (unless certain conditions are met), and any use requires careful consideration including a privacy impact assessment. It is not envisioned that the Trustee is likely to use automated decision making.

## 17. PENALTIES AND CONSEQUENCES

17.1 Breach of data protection law has consequences. Any failure to comply with this Policy puts us at risk of breaching data protection law. Sanctions can include:

(a) the imposition of material fines by the Information Commissioner's Office;

(b) criminal sanctions through the courts; or

(c) civil action by data subjects or those representing them (such as consumers' associations).

17.2 There is also the possibility of adverse publicity and/or reputational damage in relation to such issues as a breach of the security of the data.

17.3 It is therefore very important that all Trustees adhere to this Policy. If in any doubt as to the data protection implications of any proposed activity, the Trustees must take appropriate advice.

## APPENDIX

## PRIVACY NOTICE