THE AON RETIREMENT PLAN (THE "PLAN")
GENERAL DATA PROTECTION REGULATION POLICY (THE "POLICY")

1. INTRODUCTION

1.1 The General Data Protection Regulation (EU) 2016/679 as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (as amended by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the Data Protection Act 2018 (together the "**GDPR**") is designed to enhance privacy laws across Europe and came into force on 25 May 2018. The GDPR replaced all data protection legislation in EU member states (including the UK Data Protection Act 1998).

1.2 This GDPR Policy should be read in conjunction with:

1.2.1 the Record of Processing Activities (Appendix 1);

1.2.2 the Privacy Notice (Appendix 2);

1.2.3 the Data Security Breach Management Policy (Appendix 3); and

1.2.4 the Data Protection Impact Assessment (Appendix 4).

1.3 The trustee of the Plan (the "**Trustee**") will be determining the purposes and means of processing personal data held for the purposes of the Plan ("**Plan Personal Data**") and as such will be Data Controller for GDPR purposes, particularly in regard to Plan members and their beneficiaries.

1.4 This Policy explains the Trustee's procedures and processes for ensuring compliance with the overarching principles of the GDPR, both generally, and in respect of any "conditions" relied upon under UK data protection laws. This Policy also explains the Trustee's policies on the retention and erasure of Plan Personal Data both generally and in respect of any "conditions" or lawful bases of data processing relied upon under UK data protection laws.

1.5 The Trustee has taken legal advice on its duties and on the lawful bases of data processing by or on behalf of the Trustee and that advice is reflected in this Policy.

1.6 This Policy forms a part of the Trustee's obligation to demonstrate accountability.

1.7 Defined terms where used in this Policy shall have the same meaning as under the GDPR unless otherwise stated.

2. THE TRUSTEE'S ROLE

2.1 As Data Controller, the Trustee must act in accordance with the principles of the GDPR. In summary, these include ensuring that Plan Personal Data:

2.1.1 is processed lawfully, fairly and in a transparent manner;

2.1.2 is collected for specific, explicit and legitimate purposes, and not further processed in a manner that is inconsistent with those purposes;

2.1.3 is processed in a manner that is limited to the relevant information necessary for the purposes of the processing;

2.1.4 is actively managed to ensure it is accurate, or is erased;

2.1.5 is held for a limited period of time and once the purposes for which the Plan Personal Data are completed, it is no longer stored; and

2.1.6 is processed in a way that ensures security of the Plan Personal Data.

2.2 In order to carry out its duties in respect of the Plan under the GDPR, the Trustee relies on a number of third parties (including the Plan's administrator, currently Aon Solutions UK Limited (the "**Administrator**")), to administer the Plan appropriately and in accordance with its governing documentation. The Trustee has taken steps to establish that the Administrator and other third parties who process Plan Personal Data on behalf of the Trustee ("**Data Processors**") also adhere to the overarching principles of the GDPR as set out in paragraph 2.1 of this Policy. This includes ensuring that contracts entered into with Data Processors comply with the requirements of Article 28 of the GDPR.

3. DATA MAPPING AND RECORD KEEPING

3.1 In order to identify the Plan Personal Data it controls, the Trustee has carried out a data mapping exercise, which has included making enquiries of and carrying out due diligence on all Plan third party service providers who process Plan Personal Data. This included sending an initial questionnaire to each service provider to ascertain whether they considered themselves to be a data processor or data controller with a subsequent more detailed questionnaire for Data Processors. The Trustee has recorded the results of this exercise in its Record of Processing Activities, which is appended to this Policy at Appendix 1.

3.2 Read together, this Policy (including its appendices), the written legal advice received by the Trustee as referred to in paragraph 4.1 and the Record of Processing Activities are designed to comply with the requirements of Article 30 of the GDPR.

4. LAWFULNESS OF PROCESSING

4.1 The Trustee acknowledges that in order to process Plan Personal Data, it must have a lawful basis as set out under the GDPR for doing so. The Trustee has taken legal advice in respect of the Plan's regular day-to-day processing and has identified the lawful bases for processing Plan Personal Data. The Trustee is relying on the fact that the processing of Plan Personal Data is necessary:

4.1.1 for compliance with a legal obligation to which the Trustee is subject; or

4.1.2 to meet a legitimate interest of the Trustee or a third party.

4.2 When considering legitimate interests, the Trustee acknowledges that these interests must be balanced against the interests or fundamental rights and freedoms of the Data Subject (i.e. anyone about whom the Trustee holds personal information, including members, beneficiaries and potential beneficiaries).

4.3 When special categories of data (such as data in respect of health or sexual orientation) ("**Special Categories Data**") are being processed, the Trustee shall rely on the condition of the GDPR which allows Special Categories Data to be processed provided the processing is necessary for the establishment, exercise or defence of legal claims. Alternatively, the Data Protection Act 2018 permits the Trustee to process Special Categories Data and data relating to criminal convictions when performing its legal obligations in connection with employment, social security or social protection. The Trustee will rely on whichever of these two conditions applies in respect of Special Categories Data already held by the Plan even if at the time the data was collected the data subject was asked to give consent.

4.4 Where neither of the conditions referred to in 4.3 apply to the processing of Special Categories Data or data relating to criminal convictions, the Trustee may need to obtain the Data Subject's express consent to the processing. Where the Trustee is relying on the consent of a Data Subject

it will ensure that the request for consent is clearly distinguishable from other matters and that the Data Subject is informed of their right to withdraw consent at any time (which is stated in the Plan's Privacy Notice) and the Trustee will facilitate any withdrawal of consent. The Trustee will also request the Administrator to keep a copy of each consent obtained.

5. FAIR AND TRANSPARENT PROCESSING

5.1 The Trustee has (subject to paragraph 5.2 below) issued a privacy notice to Plan members reflecting the requirements of the GDPR. The privacy notice has also been published on the Plan's website, with a link from every page. A copy of the privacy notice is appended to this Policy at Appendix 2.

5.2 Where the Trustee does not have a current address for any member the Trustee acknowledges that the privacy notice will not have been provided to the member. However, the Trustee is satisfied that the steps taken by the Administrator to maintain accurate contact details for members mean that all reasonable efforts have been made to issue the privacy notice to such members.

5.3 Whilst noting that each data controller is responsible for its own compliance with the GDPR, the Plan's privacy notice is intended to cover all Data Controllers in relation to Plan Personal Data.

5.4 The Trustee understands that where it is provided with Personal Data concerning a member's family or dependants (such as in an expression of wishes form ("**EoW Form**")) it is required by Article 14 of the GDPR (subject to the exception referred to in paragraph 5.5 below) to issue a privacy notice to those individuals. The Trustee considers that strict compliance with this requirement would cause difficulties as it would require the Trustee to contact every potential beneficiary named in every EoW Form even before the member's death. Issuing a form to each potential beneficiary could substantially increase the risk of premature complaints from potential beneficiaries and could drive negative behaviours by members (such as not completing an EoW Form, or completing it in a way that does not genuinely reflect the member's wishes).

5.5 The Trustee understands that Article 14 of the GDPR contains an exception that allows a Data Controller not to issue a privacy notice where compliance with the obligation "is likely to render impossible or seriously impair the achievement of the objectives of that processing". The Trustee considers that it is reasonable to rely on this exception, and not send a privacy notice to potential beneficiaries at the time that the member submits an EoW Form because the difficulties outlined in 5.4 above would seriously impair the purpose for which the personal data is provided (being the opportunity for a member, on a confidential basis, to inform the Trustee of his wishes and to enable the Trustee to pay the correct benefits to the correct person without undue delay). As a result, the Trustee has decided not to provide a privacy notice to individuals named on an EoW Form at any point before the death of the relevant member. In taking that approach the Trustee has considered the rights and interests of those individuals and the fact that the Trustee does not ask for Special Categories Data in relation to those individuals.

5.6 There may be other circumstances where the Trustee receives Personal Data from an individual who is not the Data Subject (for example, when considering a complaint under the Plan's Internal Dispute Resolution Procedure). In such cases, the Trustee will take action on a case-by-case basis. The Trustee will consider whether providing such Data Subjects with a privacy notice will render impossible or seriously impair the achievement of the objectives of that processing (for example, to give due consideration to the complaint under the Plan's Internal Dispute Resolution Procedure). If none of these applies, the Trustee will provide a privacy notice to such Data Subjects.

5.7 A privacy notice should be sent to relevant potential beneficiaries where the Trustee is carrying out a fact find following a member's death. The Administrator has agreed with this approach.

5.8 The Trustee has put in place a process to keep the privacy notices it seeks to rely on under review and acknowledges that revised or further privacy notices will be required in certain circumstances, for example where the purpose of its processing of Plan Personal Data changes and where a non-member provides personal data as part of an application under the Plan's internal dispute resolution procedure.

5.9 The Trustee understands that Plan Personal Data may from time to time be transferred outside the UK. The Trustee has contractually obliged its third party advisers to have appropriate safeguards and technical measures in place when transferring Plan Personal Data outside the UK and has assessed whether international data transfers are necessary and proportionate as part of the Data Protection Impact Assessment.

6. STORAGE AND RETENTION OF PERSONAL DATA

6.1 The Trustee acknowledges that the principles of the GDPR require personal data to be kept for no longer than is necessary for the purposes for which it is processed and the personal data should be limited to that which is required for that purpose.

6.2 The Trustee considers that its policy for retention and erasure of Plan Personal Data must be determined in the context of its legal obligations as Trustee of the Plan and the fact that pension benefits are paid out over a very long period and that members, former members and their survivors may query a calculation or entitlement to benefits many years after settlement of the benefit. The Trustee is also under legal obligations, including HMRC requirements, to retain certain data for a number of years.

6.3 As a result, the Trustee considers it appropriate to keep Plan Personal Data (including Special Categories Data and data relating to criminal convictions) for at least 7 years after a member's benefits are finally settled – e.g. on their death or the transfer out of their benefits – and certain key elements of member data may be kept for so long as the Plan exists.

6.4 The Trustee has discussed the retention of Plan Personal Data with the Administrator. The Trustee understands that when a member's benefits are finally settled, Aon's systems do not allow member data to be rationalised so that unnecessary elements of data are deleted leaving only the key items required. Nonetheless, the Trustee understands that Aon implement appropriate technical and organisational measures to protect member data such that the risks to the data subject of retaining unnecessary data are appropriately minimised and the Trustee considers those risks to be outweighed by the need to retain key data and the systems limitations which prevent partial deletion.

6.5 The Trustee has reviewed the contractual terms for each Data Processor of Plan Personal Data and each Data Controller or joint Data Controller (as listed in the Record of Processing Activities) and considers that the contractual terms contain appropriate provisions relating to retention of data, including following termination of the appointment. In particular, the Trustee has agreed that Aon can keep a copy of plan data for up to 7 years or longer if it considers necessary following termination of its appointment as Administrator.

6.6 The Trustee has written to those former third party service providers which it believes may hold Plan Personal Data as Data Processor on behalf of the Trustee and asked them to return or destroy it. Those letters and their replies are included in the Record of Processing Activities.

6.7 The Trustee has written to former trustee directors who have retired since the date of the merger in 2012 and trustees of the legacy schemes at the time of the merger in order to inform them of the requirements of the GDPR and to ask them to return or destroy any Plan Personal Data which they still hold. Those letters and their replies are included in the Record of Processing Activities.

6.8 On leaving office each departing trustee director will be required to return or destroy any Plan Personal Data they hold.

7. SECURITY OF PROCESSING

7.1 The Trustee is aware of the standard of security and appropriate technical and organisational measures required under the GDPR. The Trustee has taken into account such factors as the costs of implementation of that security, the nature, scope, context and purposes of processing and the risk of the varying likelihood and severity for the rights and freedoms of Data Subjects to ensure a level of security appropriate to such risk in respect of its processing of Plan Personal Data.

7.2 In particular, the Trustee has put in place the following measures:

7.2.1 the Trustee has agreed that wherever possible papers and materials circulated to/from the Trustee and its advisers which contain personal data will not also contain the name of the data subject;

7.2.2 all papers and materials circulated to/from the Trustee and its advisers which contain Personal Data will be password protected;

7.2.3 each Trustee Director's iPad is suitably password protected;

7.2.4 the Trustee has received confirmation from Aon that it, as Administrator, holds a Record of Processing Activities which details the activities it performs for the Trustee; and

7.2.5 data security issues have been added to the Plan risk register.

7.3 The Trustee is satisfied that at the date of this Policy, it meets the security of processing requirements set out under the GDPR, and shall keep such measures under ongoing review.

7.4 The Trustee has contractually obliged the relevant parties identified in the Record of Processing Activities to meet the security measures under the GDPR on an ongoing basis. In line with the ICO's Data Sharing Code of Practice, whenever sharing data with another Controller, the Trustee will consider putting in place a written data sharing agreement.

8. TRUSTEE INTERNAL PROCEDURES AND SECURITY

8.1 Each trustee director has committed to keeping all Plan Personal Data confidential.

8.2 Each trustee director will access Plan Personal Data only on the iPad issued or authorised by the Trustee.

8.3 Each trustee director should not access Plan Personal Data when outside the UK unless it is absolutely necessary to fulfil legal obligations. Where Plan Personal Data is accessed from outside the UK the trustee director should take appropriate steps to ensure the security of both the device used and the method of access.

9. DATA BREACHES

9.1 The Trustee recognises the authority of the Information Commissioner's Office (the "**ICO**") and it intends to cooperate on request with the ICO. The Trustee recognises its obligation to inform the

ICO of certain personal data breaches within 72 hours of becoming aware of them, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of Data Subjects.

9.2 The Trustee's Data Security Breach Management Policy is appended to this Policy at Appendix 3.

10. DATA SUBJECT RIGHTS

10.1 The Trustee acknowledges that Data Subjects are granted rights in respect of their personal data, including the right:

10.1.1 to receive privacy notices;

10.1.2 to access their personal data and relevant further information;

10.1.3 to correct inaccurate or incomplete personal data;

10.1.4 to 'be forgotten' (i.e. to have personal data erased);

10.1.5 to restrict processing of personal data;

10.1.6 to receive a copy of their personal data or transfer their personal data to another data controller;

10.1.7 to object to processing of personal data;

10.1.8 not to be subject to automated decision-making; and

10.1.9 to receive notification of a Personal Data Breach where it is likely to result in a high risk to the rights and freedoms of the Data Subject, or where required to do so by the ICO.

10.2 The Trustee notes its responsibility to provide any communication, or take any actions, requested by a Data Subject in exercise of the rights referenced above, free of charge, except on the rare occasion where such requests are unfounded or excessive.

10.3 The Trustee has agreed with the Administrator to put in place appropriate processes to meet those rights.

11. DATA PROTECTION IMPACT ASSESSMENT ("DPIA")

The Trustee has carried out a DPIA. This is attached at Appendix 4 to this Policy.

12. DATA PROTECTION OFFICER

The Trustee has taken legal advice and, in light of that advice, does not believe that it is required under the GDPR to appoint a Data Protection Officer at this time, but is committed to keeping the position under review.

13. REVIEW OF POLICY

13.1 The Trustee shall carry out a regular review of the decisions set out in this Policy and, when necessary and with regard to any supplementary guidance introduced by the ICO, shall issue a revised policy.

13.2 The Trustee shall ensure that the Policy and its compliance with the GDPR are reviewed each time a new third party adviser is appointed to provide services to the Plan, or in the event that a new system is adopted.

13.3 To assist with the Trustee's regular review of this Policy, this Policy has been added to the Trustee's risk register.

13.4 The Trustee reserves the right to amend this Policy from time to time.

Policy Adopted: 25 May 2018

Policy revised and readopted: July 2019

Policy revised and readopted: June 2020

Policy revised and readopted: 2 September 2021

Policy revised and readopted: 13 May 2022

Policy revised and readopted: 18 September 2024

Appendix 1: Record of Processing Activities

The following record of processing activities is a summary of provider and processing status; a more detailed table is maintained by the Secretariat and is available for review if required.

Provider	Section	Service	Status
Aon	All Sections	Actuarial	Data controller
Aon	All Sections	Administration	Data processor
Aon	All Sections	Secretariat	Data processor
Aviva	A&A Annuity	Annuity Provider	Data controller
Canada Life	A&A Annuity	Annuity Provider	Data controller
CMS Cameron McKenna Nabarro Olswang LLP	All Sections	Legal Adviser	Data controller
EY	All Sections	Auditor	Data controller
Icon Collections	All Sections	Debt Collection	Data Processor
JUST	HPF Annuity	Annuity Provider	Data controller
Origen	All Sections	Financial Adviser	Data controller
Phoenix	A&A annuities	Annuity Provider	Data controller
PIC	A&A Annuity Aon UK Annuity HPF Annuity	Annuity Provider	Data controller
Rothesay	Aon UK Annuity Aon Bain Hogg Annuity	Annuity Provider	Data controller
Reassure	A&A Annuity	Annuity Provider	Data controller

Provider	Section	Service	Status
Scottish Widows	Aon Bain Hogg Annuity (Policy M97D)	Annuity Provider	Data controller
Standard Life	Bain Hogg Annuity	Annuity Provider	Data controller
Utmost Life and Pensions	A&A Annuity	Annuity Provider	Data controller
Zurich	Aon Bain Hogg Annuity	Annuity Provider	Data controller

Appendix 2: Privacy Notice

AON RETIREMENT PLAN: PRIVACY NOTICE

Aon UK Trustees Limited (the "**Trustee**") holds and uses personal information about Plan members and beneficiaries to run the Aon Retirement Plan (the "**Plan**"), in line with the 'data protection' laws in force at the time.

What we do with your information

The Trustee is a 'data controller'. This means the Trustee collects and uses your personal details to meet its legal duties, and for other legitimate purposes solely to do with running the Plan. These may include:

- calculating, managing and paying Plan benefits to you, or following your death;
- dealing with any queries, complaints or appeals about decisions we have made, for example about the Plan benefits you or your dependants are entitled to receive; and
- meeting legal requirements and best practice.

We have received much of the information we hold from the members themselves. You may have also given us details about your beneficiaries – that is, people who may be eligible to receive benefits after your death. We assume that you have your beneficiaries' consent to give us this information and that you will share this privacy notice with them.

However, in certain circumstances we also hold and use information provided by:

- Aon UK Limited and Aon Solutions UK Limited, the sponsoring employers of the Plan (the "**Plan Employers**");
- other employers or pension schemes associated with the Plan Employers or the Plan;
- medical advisers;
- any pension scheme or arrangement where you had benefits which you then transferred to the Plan;
- HM Revenue & Customs;
- the Department for Work and Pensions;
- regulatory bodies (such as the Pensions Regulator); and
- tracing services.

The information we hold

The details about you that we use to help us calculate and pay your benefits include:

- full name, date of birth, National Insurance number (or any other official ID numbers);
- business and personal contact details, including address, telephone numbers and email addresses;
- financial information, including salary, pension or prospective pension entitlement and bank account details;
- employment details, including years of service, employment start and leave date;
- your pension benefit choices, including any you may make online through the Plan portal; and

- marital or relationship status, including your beneficiaries' full names, dates of birth, contact details and relationship to you.

We also hold and, in appropriate circumstances, use particularly 'sensitive' data about you – for example, to allow us to manage any ill-health or death benefits. We will normally process this information in the performance of our legal obligations in connection with employment, social security and social protection (as allowed by legislation). We may also, generally when considering claims under the Plan's Internal Dispute Resolution Procedure, process any sensitive data for the purposes of establishing, exercising or defending legal claims. If we ask for your explicit consent to do this then you can withdraw this consent at any time.

Sharing your information

Where appropriate, we share your personal details with certain third parties involved in running the Plan, this includes:

- the Plan administrator (and its administration and website system providers who may hold some of those personal details centrally in respect of all accounts held with that provider);
- the Plan actuary and their support team;
- the Plan Employers and their advisers;
- buy-in providers and similar providers to assess future provision of benefits outside the Plan (including those with whom the Trustee has already secured certain benefits in the Plan), together with their reinsurers and third party administrators;
- other persons responsible for providing or communicating benefits, e.g. occupational health service providers.

We may also make information about you available to:

- any other companies associated with the Plan Employers – for example, to firms which may buy (or have already bought) part or all of the Plan Employer's business;
- the trustee, sponsoring employer, administrators or professional advisers of any pension scheme you may have transferred benefits to or from.

We can also share your personal information outside the Plan if you ask us to, or if we need to respond to or comply with a judicial proceeding, court order, request from the Pensions Regulator, Pensions Ombudsman or any other regulator or any other legal process served on or involving the Trustee.

In some situations, we share responsibility for your personal details with the Plan actuary, the legal advisers (who need information about you to carry out their professional duties to the Trustee), insurers and the auditors.

In turn, the Plan Employers use your details to meet their legal obligations as the sponsoring employers of the Plan. They have a legitimate interest in managing Plan costs and may want to offer certain options to members.

The Buy-in Providers process some members' data as a data controller to take steps necessary for the buy-in insurance policies and to provide data to their reinsurers, administer the buy-in policies and comply with applicable laws and regulations.

Please note that the Plan Employers, the Plan Administrator, the Buy-in Providers and other advisers receiving your personal details may sometimes pass information to other countries. When this happens, they must make sure that the party receiving the information has proper security measures in place including appropriate contractual arrangements.

Storing your personal data

Pension benefits are payable over a long period and your right to benefits from the Plan may depend on information going back many years. We keep the information we hold about you throughout your membership of the Plan. Once your membership ends, we will decide whether to delete some of these details after 7 years. However, we may hold information for longer if necessary to make sure the Plan pays the correct benefits and to deal with any queries about your benefits which may arise after that time.

Aon Solutions UK Limited, as the Plan Administrator, will hold on to your personal details for 7 years after the termination of the contract with us or for longer if necessary in order to protect themselves against any later legal claims.

Where the Buy-in Providers hold your personal data, they will retain this for as long as they consider necessary in order to comply with their legal and regulatory obligations and to protect themselves against any subsequent legal claims.

Your rights

You have the right to see the information we hold about you. You can ask us to correct any mistakes, or erase some or all of the details we have.

In some situations, you can ask us to limit the way we use your personal information, object to our using it at all, or request a copy of it to share elsewhere.

Where you have given us your consent to use particular information, you can withdraw that consent at any time. However, please bear in mind that if we do not hold all the details we need, we may not be able to pay out the benefits you are entitled to.

You may view the Aon Solutions UK Limited Privacy Notice online at https://www.aon.com/unitedkingdom/retirement-investment/retirement-investment-services-privacy-statement.jsp

Contact details

If you have any questions or want to know more about the information the Trustee holds and why, or about the Plan's 'data protection' arrangements, please contact Andrew Timms at:

Address: Aon Solutions UK, Briarcliff House, Kingsmead, Farnborough, Hampshire, GU14 7TE

Email: andrew.timms@aon.com

Issues and complaints

To make a complaint about how we've handled your information, contact us as set out above.

If you're not satisfied with our response to your complaint or believe our use of your information is not in line with data protection law, you can make a complaint to the Information Commissioner's Office. Its contact details are:

Address: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Telephone number: 0303 123 1113 or 01625 545 745

Appendix 3: Data Security Breach Management Policy

The Aon Retirement Plan (the "Plan")
Personal Data Breach Management Policy

1. BACKGROUND

1.1 The General Data Protection Regulation (EU) 2016/679 as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (as amended by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the Data Protection Act 2018 (together, the "**GDPR**") requires pension scheme trustees to implement appropriate technical and organisational measures to ensure a level of security for the personal data it holds *"appropriate to the risk, including… the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident".*

1.2 The GDPR also requires that where a breach does occur, the data controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, *"notify the personal data breach to the supervisory authority… unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."*

1.3 If the personal data breach is likely to result in a "*high risk to the rights and freedoms*" of the data subject, the GDPR requires trustees to communicate the personal data breach to the data subject *"without undue delay."*

1.4 The Guidelines on Personal Data Breach Notification adopted on 6 February 2018 and endorsed by the European Data Protection Board on 25 May 2018 are taken into account in this Policy as is relevant guidance issued by the Information Commissioner's Office (the "**ICO**") (together referred to as the "**Guidance**").

1.5 In addition, the operation of the Plan is heavily reliant on information technology and automated processes and so the Plan is exposed to cyber security risk. In particular, the Plan is exposed to the risk of external intervention in the operation of the Plan where there is a criminal motive. Whilst that intervention may involve personal data, and so come within the scope of the GDPR, the intervention might be operational rather than data related (e.g. the use of ransomware to block Plan administration or investment activity).

2. OBJECTIVES

2.1 The purpose of this Policy is to establish what action Aon UK Trustees Limited (the "**Trustee**") should take in response to any reported personal data breach incident and ensure that any breach is appropriately logged, managed and, where appropriate, reported to the ICO and the data subjects (being Plan members, beneficiaries and potential beneficiaries as appropriate) (the "**Data Subjects**").

3. IDENTIFYING A PERSONAL DATA BREACH

3.1 A personal data breach (a "**Breach**") is:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

3.2 Examples of Breaches could include, but are not limited to:

3.2.1 loss of data or equipment on which the data is stored;

3.2.2 unauthorised access to that data;

3.2.3 equipment failure;

3.2.4 human error in handling data;

3.2.5 unforeseen circumstances such as fire or flood;

3.2.6 hacking attacks; and

3.2.7 offences where information is obtained by deception.

3.3 The Trustee will seek to ensure that the contractual terms agreed with their third party advisers who receive Plan personal data confirm the legal obligation on those parties to notify the Trustee (and the ICO where required) of a Breach without undue delay.

3.4 A "**Cyber Breach**" means disruption or damage to the Plan or its members as a result of the failure of information technology systems and processes operated by or on behalf of the Trustee. This might include:

3.4.1 equipment failure;

3.4.2 business continuity failure preventing access to information technology systems; and

3.4.3 the use of ransomware and other criminal activity to block the operation of the Plan's information technology systems and processes.

3.5 The Trustee will seek to ensure that the contractual terms agreed with their third party advisers, who are Data Processors, and who receive Plan personal data confirm the legal obligation on those parties to notify the Trustee of a breach without undue delay.

4. PERSONAL DATA BREACH RESPONSIBILITY

4.1 The Trustee will maintain a data protection log in which to record all incidents of Breaches (or suspected Breaches) in accordance with this Policy.

4.2 The Trustee has appointed a Breach response team (the "**DP Team**") consisting of at least two members of the Governance, Risk and Audit Sub-Committee from time to time and a Company Representative.

4.3 Confirmed or suspected Breaches should be reported promptly to the Secretary to the Trustee, Andrew Timms (andrew.timms@aon.com, 01252 768 033) (the "**DP Contact**").

4.4 When a confirmed or suspected Breach is reported, the DP Contact will arrange a conference call with all available members of the DP Team, the reporter of the Breach and any other person who the DP Contact believes may assist in dealing with the Breach. This call will be arranged as soon as practical after the DP Contact receives a report and, wherever feasible, within 24 hours of the report being received.

4.5 The DP Team will take into account the Guidance when considering a confirmed or suspected Breach and the appropriate response to it.

5. INFORMATION GATHERING

5.1 The DP Team will investigate the suspected Breach and, where it has established with a reasonable degree of certainly that a Breach has occurred, prepare a data breach report which should include the following information where possible:-

5.1.1 a description of the suspected Breach;

5.1.2 the time the suspected Breach was identified and by whom;

5.1.3 name and contact details of the reporter;

5.1.4 the volume of data involved, to include where possible the categories and approximate number of Data Subjects and personal data records concerned;

5.1.5 whether the Breach has been contained or is ongoing

5.1.6 the likely consequences of the Breach;

5.1.7 where appropriate, what actions are or can be taken to recover data; and

5.1.8 who else is known to be aware of the Breach.

5.2 The DP Team should assess the risk to Data Subjects by considering:-

5.2.1 whose data is affected – e.g. individual member, groups of members?

5.2.2 does the Breach involve Special Categories Data – e.g. health information or information identifying sexual orientation?

5.2.3 is the data otherwise particularly sensitive – e.g. does it include bank details?

5.2.4 what could any data lost tell a recipient about the individual – e.g. could it assist in identity fraud?

5.2.5 what potential harm could be caused to individuals – e.g. financial, reputational, emotional wellbeing, fraud, identity theft or damage or delay in benefit processing?

6. CONTAINMENT AND RECOVERY

6.1 The DP Team will endeavour to:

6.1.1 identify the cause of the Breach;

6.1.2 establish what steps can or need to be taken to contain the Breach;

6.1.3 contact all relevant persons (subject to any confidentiality obligations) who are or may be able to assist in the process, or who have a right to be informed or consulted, and take advice where appropriate;

6.1.4 determine what can be done to recover the breach – e.g. recovery of data, use of back-up data; and

6.1.5 consider informing appropriate third parties (for example the police and banks and any contractual counterparty who has a right to be informed or consulted).

6.2 In relation to a Cyber Breach, the Breach Team will establish what steps can be taken to restore normal operation of the Plan including:

6.2.1 monitoring the implementation of business continuity arrangements;

6.2.2 considering the risks arising from any steps taken to restore normal operation; and

6.2.3 granting any necessary approvals for a return to normal operation.

6.3 The DP Team will record all breaches, comprising the facts relating to the breach, its effects and the actions in the data protection log.

7. COMMUNICATION

7.1 The DP Team will determine whether or not the Breach *"is likely to result in a risk to the rights and freedoms of"* the Data Subjects. If the DP Team determines that it is then it will submit a

report (the "**Report**") to the ICO (copied to the Trustees) without undue delay and where feasible within 72 hours of establishing with a reasonable degree of certainty that a Breach has occurred.

7.2 The Report should include as a minimum:-

7.2.1 a description of the nature of the Breach;

7.2.2 the categories and approximate number of Data Subjects concerned and data records affected;

7.2.3 contact details of the DP Contact (and/or the DP Team); and

7.2.4 a description of the likely consequences of the Breach and the measures taken or proposed to be taken to address the Breach including mitigation of its possible adverse effects.

7.3 If the DP Team determines to submit a Report under 7.1 above but is unable to include all the information set out in 7.2 above then it will provide the ICO with partial information (and reasons as to why it cannot provide all the required information) within the 72 hour timeframe and provide other information as it becomes available and without undue delay.

7.4 The DP Team will determine whether in its view the Breach is likely to result in high risk to the rights and freedoms of Data Subjects. If so, it will communicate information about the Breach to affected Data Subjects without undue delay.

7.5 The communication to Data Subjects should be in clear and plain language and include as a minimum:-

7.5.1 a description of the nature of the Breach;

7.5.2 relevant contact details for the Plan;

7.5.3 a description of likely consequences of the Breach;

7.5.4 a description of the measures taken or proposed to be taken by the Trustee to address the Breach, including measures to mitigate its possible adverse effects; and

7.5.5 where appropriate, specific advice to individuals to protect themselves from possible adverse consequences, e.g. resetting passwords.

7.6 The DP Team will consider the most appropriate form of communication to affected Data Subjects, e.g. email, text, or written correspondence, taking into account the immediacy or severity of any risk. It should also consider whether any general notification should be made to members and if so, in what form.

7.7 Before submitting any Report or communicating with Data Subjects or the ICO or any third party, the DP Team will consider the parties they are obliged to notify or consult with and take appropriate steps.

7.8 Subject to 7.7 above, the DP Team has authority to determine which persons need to be notified or communicated with and the terms of any notice or communication.

7.9 The DP Team will, where considered appropriate, consult the ICO on the content and method of any communication with Data Subjects.

7.10 If, after submitting the Report to the ICO, the DP Team receives evidence that the security incident was contained and no Breach actually occurred then it shall notify the ICO of this.

7.11 Where any breach, including a Cyber Breach, has resulted in the failure of the Trustee to comply with any legal obligation, the Breach Team will also consider the need to report the breach to the Pensions Regulator.

8. REVIEW

8.1 In the event of a Breach and following necessary actions being taken by the DP Team in accordance with this Policy, the DP Team will:

8.1.1 having submitted such reports and communications as above, revisit the situation and re-evaluate communications and developments in case there are any subsequent communications or notifications which need to be made;

8.1.2 record all Breaches, including the facts relating to the Breach, its effects and the actions taken in the data protection log;

8.1.3 prepare a report for the next Trustee meeting and ensure that the data protection log is updated including reasons for informing the ICO or Data Subjects, or for not doing so; and

8.1.4 review the data sharing arrangements in place and consider if any changes are necessary.

8.2 At the next Trustee meeting following the Breach, the Trustee will consider whether any further investigation of the breach is required. The Trustee will also note any lessons to be learnt from the Breach, including communication with appropriate data processors and other third party advisers accordingly.

8.3 The Trustee will carry out a regular review of this Policy and, where appropriate (including having regard to any supplementary guidance from the ICO), will issue a revised Policy.

8.4 The regular review of this Policy has been added to the Trustee's risk register.

Policy adopted: May 2018

Policy revised and readopted: June 2020

Policy revised and readopted: 2 September 2021

Policy revised and readopted: 13 May 2022

Policy revised and readopted: [5 May 2023]

Appendix 4

DATA PROTECTION IMPACT ASSESSMENT

1. INTRODUCTION

1.1 The Trustee has carried out this Data Protection Impact Assessment ("**DPIA**") in compliance with Article 35 of the GDPR. In producing this DPIA, the Trustee has considered and taken advice on WP29 guidelines and ICO guidance on DPIAs.

1.2 The Trustee does not consider that the processing of Plan Personal Data by or on behalf of the Trustee is likely to result in a high risk to the rights and freedoms of natural persons. However, the Trustee acknowledges that it does (or may):

1.2.1 process sensitive data;

1.2.2 process data on a large scale;

1.2.3 process data concerning vulnerable data subjects (which may include the elderly or children);

1.2.4 transfer data (or permit the transfer of data) outside the UK;

1.2.5 process "invisible data" (as described by the ICO as processing personal data which has not been obtained direct from the Data Subject, in circumstances where it has determined not to issue a privacy notice in accordance with paragraphs 5.4 - 5.6 of the Policy).

1.3 Given this processing activity and the ICO's guidance, the Trustee has decided that even if it may not be required in these circumstances under the GDPR, it would be good practice to undertake a DPIA.

2. DESCRIPTION OF THE PROCESSING

2.1 In order to identify the Plan Personal Data it controls, the Trustee has carried out a data mapping exercise, which has included making enquiries of and carrying out due diligence on all Plan third party service providers who process Plan Personal Data. See section 3 of the Policy.

2.2 A summary of the types of data held by the Plan is given in Trustee's Privacy Notice which is attached to the Policy.

2.3 The Trustee may hold Special Categories Data including relating to health and sexual orientation and data relating to criminal convictions. An explanation of this processing and the lawful basis for it is set out in section 4 of the Policy.

2.4 The Plan has approximately 13,400 members and beneficiaries, the vast majority of whom live in the UK. The Trustee therefore acknowledges that the processing of Plan Personal Data could be considered to be carried out on a large scale.

2.5 The purpose of the processing and its intended effect is necessary to enable the Trustee to perform its legal obligation to properly administer the Plan and pay the benefits due under it. The Trustee considers that this processing is in the interests of members and beneficiaries. The form of processing is not novel and the Trustee considers that Plan members and beneficiaries would expect and understand that their personal data will be processed, on a lawful basis, in order to provide for the payment of their Plan entitlements. There are no known concerns over this type of processing or security flaws.

3. CONSULTATION PROCESS

3.1 The Trustee considered whether Plan members and beneficiaries should be consulted about the processing of Plan Personal Data. The Trustee concluded that such consultation would not assist with the conduct of the DPIA and would be disproportionate and impractical.

3.2 The Trustee has consulted with the Administrator, who has assisted in producing this DPIA as appropriate.

3.3 The Trustee has also consulted with the employer.

4. ASSESSMENT OF NECESSITY AND PROPORTIONALITY

4.1 The Trustee's lawful basis for processing is set out in section 4 of the Policy. The Trustee considers that the processing carried out by or on behalf of the Trustee is necessary and proportionate in the context of the stated lawful basis.

4.2 The Trustee's policy on data minimisation and retention is set out in section 6 of the Policy. The Trustee considers that the long term retention of data in relation to Plan members and beneficiaries, including after the individual has ceased to be a Plan member or beneficiary, is legitimate and justified, and does not carry any significant risk to the data subject.

4.3 The information provided to Data Subjects is set out in the Privacy Notice at Appendix 2 to the Policy. The Trustee considers that the Privacy Notice provides a concise and transparent explanation of the processing carried out by or on its behalf.

4.4 The Trustee has entered into contracts with Data Processors in compliance with Article 28 of the GDPR as confirmed in paragraph 2.2 of the Policy. The Trustee has, wherever possible, also put in place suitable contractual arrangements where the Trustee shares data with other Data Controllers, including joint controllers.

4.5 The Trustee has contractually obliged its third party advisers to have appropriate safeguards in place when transferring Plan Personal Data outside the UK as set out in paragraph 5.9 of the Policy.

5. IDENTIFYING, ASSESSING AND ADDRESSING RISK

5.1 The main sources of risk identified in respect of the data processing as described in 1.2 above include:

5.1.1 Security breaches, including cyber-crime and loss of hardware;

5.1.2 Administrative error;

5.1.3 Retention and use of inaccurate personal data;

5.1.4 Processing of invisible data, where the data subject is unaware of that processing.

5.2 The Trustee includes cyber security in its risk register and has sufficient and proportionate controls in place to minimise the risk of a cyber incident occurring, and to reduce the impact of any breaches that do occur. The Trustee requires third party processors, particularly the Plan administrator, to have in place sufficient controls to protect Plan Personal Data. The Trustee's policy on security of processing is set out in sections 7 and 8 of the Policy.

5.3 An example of the risk of administrative error would be if the personal data of a member was sent to the wrong postal or e-mail address. This could cause the individual distress and embarrassment and potentially leave them open to identity fraud or other financial crime. The Trustee and the Plan administrator operate internal controls (as required by section 249A

Pensions Act 2004) to minimise the risk of administrative errors occurring and the Trustee considers those controls to be appropriate and proportionate.

5.4 Harm caused by inaccurate personal data could include data being sent to the wrong person (as above) or the incorrect information or benefits being given to the member. The Trustee is required by the Pensions Regulator to report annually on its measurement of data (which includes checking that Plan data is both present and accurate). The measurement of Plan data is undertaken on the Trustee's behalf by the Administrator in accordance with the contractual arrangements between them. The Trustee notes that in many cases the inaccuracy of data arises from the failure of the Plan members to inform the Trustee when their data changes. Accordingly, the Trustee has a policy to remind members at appropriate intervals of the need to keep their Plan information up to date.

5.5 In certain circumstances the Trustee processes "invisible data" (as described in 1.2.5 above). This will most often arise where holding personal data of individuals named in Expression of Wish Forms completed by members or processing information about beneficiaries following the death of a member. The Trustee has identified the main risk of harm being that the data subject is distressed when they discover that their data had been held without a privacy notice being issued and without them being informed of their rights of access to that data. However, the Trustee considers this risk not to be significant and to involve minimal harm to the data subject. Accordingly, the Trustee has concluded (as set out in 5.4 and 5.5 of the Policy) that it should not provide a privacy notice to individuals named on an Expression of Wish Form at any point before the death of the relevant member and will only take proportionate steps to provide a privacy notice to those potential beneficiaries who may be identified following the death of a member.

6. REVIEW OF DPIA

6.1 The Trustee shall review this DPIA when it carries out a review of its Policy and, in addition, at any time where it considers a review to be necessary having regard to any supplementary guidance introduced by the ICO. The Trustee shall, where appropriate, issue a revised DPIA following any such review.

6.2 To assist with the Trustee's regular review of this DPIA, it has been added to the Trustee's risk register.