Find out about our policy on privacy and data protection

At Aegon, we're committed to protecting and respecting your privacy. Looking after the personal information that we collect for our employees and their dependents or beneficiaries is our top priority, and we want you to be confident that your information is in safe hands. We've developed this Fair Processing Notice to let you know:

- how and why we collect personal information;
- what we do with it;
- when and why we share it with other organisations, including the types of organisations involved;
- how long we'll keep it for, and
- the rights and choices you have when it comes to your personal information.

Contact us

If you have any questions about this notice or data protection, please contact our Data Protection Officer

Post: Data Protection Officer, Aegon, Edinburgh Park, Lochside Crescent, Edinburgh, EH12 9SE

Email: dataprotection@aegon.co.uk

How and why we obtain personal information about you

We may collect personal data relating to employees, agency or contract workers, interns, job applicants, directors or office holders.

You may give us information about yourself when completing forms (paper versions or through our website) or by contacting us by phone, email or otherwise. This includes information you provide when you:

- submit an application for a job electronically or otherwise (e.g. through a recruitment agency);
- contact us (via phone/email), or
- update Workday (our HR Information System).

We may gather information about you during the recruitment process or during your employment with us. Depending on the circumstances, the personal information we gather about you may include:

- your name;

- address;
- personal and work related contact details;
- date of birth;
- NI Number;
- marital or civil partnership status;
- next of kin and emergency contact information;
- dependents;
- gender;
- immigration and nationality;
- racial, ethnic origin;
- email address;
- phone number;
- financial information (which may include remuneration, bank details, HMRC and other PAYE or tax records);
- medical information;
- employment history, curriculum vitae, application forms, assessments, references and other recruitment information;
- holiday and absence records;
- training and performance information;
- qualifications;
- driving license details;
- details of professional memberships;
- on site CCTV and other information gathered via electronic means (which may include security system information, IT logon information);
- photographs;
- trade union membership;
- race or ethnicity;
- religious or other beliefs;
- political opinions;
- sexual orientation;
- background screening (which may include credit and criminal record information);
- any further personal information required as part of an application or which you share through the website, and

- any further personal information that we require to process during the course of your employment.

Application forms

Personal information is collected through our online application process to enable us to proceed with your application for employment with us. We'll also collect and process your personal information throughout the course of your employment with us and beyond (where applicable and in line with our retention obligations). We need this information to fulfil your contract of employment with us. Without this information we wouldn't be able to employ you.

Publicly available information

As part of our recruitment process, we may collect and use information about you that is supplied to us by recruitment partners or that is publicly available, e.g. CV from a recruitment website, or information held on social media platforms.

Workday

Holding your personal information on Workday (our HR Information System) allows you to manage your information, as well as having sight of what is held about you by Aegon. Your manager, senior management and HR will also have access to certain information to enable them to manage you and inform and support management decisions in the workplace.

We may use your information for statistical or research purposes or for testing our systems. If we do this your personal information will be anonymous so that you can't be identified.

Our data security policies mean that we hold all personal information securely and limit access to those who need to see it. We apply extra security to sensitive personal information, such as medical details.

Use of your personal information

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- When we need to perform the contract we have entered into with you
- When we need to comply with a legal obligation
- When it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests

We may also use your personal information in the following situations, which are likely to be rare:

- When we need to protect your interests (or someone else's interests).
- When it is needed in the public interest or for official purposes.

In most cases, we need the types of information listed above to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below:

- Making a decision about your recruitment or appointment
- Determining the terms on which you work for us
- Checking you are legally entitled to work in the UK
- Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance Contributions
- Providing you with statutory, contractual or non-contractual employment benefits
- Enrolling you in our pension scheme and liaising with the pension provider
- Administering the contract we have entered into with you
- Administering employment policies and procedures
- Business management and planning, including accounting and auditing
- Conducting performance reviews, managing performance and determining performance requirements
- Making decisions about salary reviews and compensation
- Assessing qualifications for a particular job or task, including decisions about promotions
- Gathering evidence for possible grievance or disciplinary hearings
- Making decisions about your continued employment or engagement
- Making arrangements for the termination of our working relationship
- Education, training and development requirements
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work
- Ascertaining your fitness to work, including provision of any workplace adjustments
- Managing sickness absence
- Complying with health and safety obligations
- To prevent fraud
- To comply with regulatory duties set by the FCA, PRA, Dutch National Bank, or other regulators
- To monitor your use of our information and communication systems to ensure compliance with our IT policies
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution

- To conduct data analytics studies to review and better understand HR and employment data (e.g. absence, attrition data)
- To promote and monitor diversity, inclusion and equal opportunities

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

We will only use your information for the purposes for which we collected it, or for reasons compatible with those purposes. If we need to use it for any other unrelated purpose then we will let you know. Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Sharing your personal information

Service providers

We work with carefully selected service providers that carry out certain functions on our behalf. These include companies that help us with:

- technology services
- background checking services
- payroll services, e.g. HMRC
- medical services, e.g. occupational health services
- outplacement services
- benefits such as Income Protection, Life Assurance, Critical Illness
- accounting, tax, legal or other advice

We only share the appropriate level of personal information necessary to enable our service providers to carry out their services and we require them to keep the information safe and protected at all times. Our service providers must only act on our instructions and can't use your information for their own purposes.

Why do we conduct background screening for employees and potential employees?

As a financial services company, the trust of customers, business partners and other stakeholders is of great importance to Aegon. This means conducting our business with integrity, openness and clarity.

To assess the integrity of all employees, Aegon performs a screening process for new candidates as well as screening when employees move to roles requiring greater levels of integrity risk. Vetting will apply across Aegon UK as part of the recruitment process for all new employees, workers, and all employees successful in applying for internal vacancies; as well as on a regular basis.

Our background checking process includes include financial sanctions checks, Politically Exposed Persons checks, credit records checks, criminal record checks (including charges for criminal offences of a financial nature) and 3 year employment reference checks.

Aegon assesses the integrity of the candidates and employees within internally set norms and values as stated in the Aegon Code of Conduct. The Money Laundering Regulations 2017 and the FCA Handbook each require firms to carry out screening of employees before their appointment and during the course of the appointment.

Sharing of special categories of personal information, for example medical information

If we request medical information from you or a medical practitioner who has cared for you or from other insurers, this will be protected. We may ask for information from other insurers or medical practitioners to check, clarify or expand answers you've given us.

Additional data sharing obligations

Other than the circumstances detailed above, we won't disclose your personal information to any third parties, except:

- to the extent that we're required to do so by law, by a government body or by a law enforcement agency, or for crime prevention purposes (including financial crime protection and credit risk reduction);
- when protecting your interests or the interests of other individuals or for reasons of substantial public interest;
- in connection with any legal proceedings (including prospective legal proceedings);
- in order to establish or defend our legal rights;
- in the event that we sell or buy any business or assets, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets, or
- if we, or substantially all of our assets, are acquired by a third party, we may disclose your personal data to that third party in connection with the acquisition.

In each case this will be done confidentially, so as to protect your personal data.

Personal information processed outside of the European Economic Area (EEA)

The personal information that we collect may be transferred to, and stored at a destination outside the European Economic Area (EEA), in connection with the above purposes.

This could be to other companies within the Aegon Group or to service providers working on our behalf. Where any such processing takes place, appropriate controls, such as the adoption of agreements containing the appropriate standard data protection clauses, are in place to ensure that your information is protected to the same standard as if it were in the UK.

Retention of personal information

We'll keep your personal information for the lifetime of your employment with us and for up to seven years after your employment ends. This is to ensure that we comply with our statutory retention obligations and legislative requirements. Further details on retention periods can be obtained from our Data Protection Officer.

Your rights

You have a number of rights under the Data Protection laws, including:

- the right to request a copy of the personal information we hold on you. When you request this information, this is known as making a Subject Access Request (SAR). In most cases, this will be free of charge, however in some limited circumstances, for example, repeated requests for further copies, we may apply an administration fee;
- the right to have personal information we hold about you transferred securely to another organisation in electronic form;
- the right to have any inaccurate personal information corrected;
- the right to have any out of date personal information deleted once there's no business need or legal requirement for us to hold it;
- the right to object or restrict some processing, in limited circumstances and only when we don't have legitimate grounds for processing your personal information;
- In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law, and
- the right to object to your personal information being used to send you marketing material. Currently HR does not conduct any direct marketing but we'd only ever send marketing material where you've given us your consent to do so.

To exercise any of these rights, please contact our Data Protection Officer on the details in the contact us section above.

Making a complaint

If you believe we haven't processed your personal information in accordance with our Data Protection obligations, and that you've been affected by our non-compliance, you can make a complaint to us by contacting our Data Protection Officer. You also have the right to ask us to

escalate your complaint to our Group Data Protection Officer if you don't think it's been handled appropriately.

If you're not satisfied with our response, you can raise a complaint with the Information Commissioner's Office, the UK's independent authority set up to enforce the Data Protection Regulations.