For customers

Protecting your personal information

Aegon's privacy notice

We keep our privacy notice under regular review. This privacy notice was last updated February 2025.

If your personal circumstances mean you need any additional support, or if you'd like a large print, Braille or audio version of this document, please visit **aegon.co.uk/additionalsupport**

Contents

Introduction

Here at Aegon, we're committed to protecting and respecting your privacy. Looking after the personal information that we collect about individuals is our top priority. We want you to be confident that your information is in safe hands and only collected and used in accordance with applicable laws and regulation, so, we've developed this Privacy notice to explain how we use the personal information that we collect in relation to our retirement, investment, savings and protection products and services.

Most personal information we collect relates to the individuals who take out a product with us. However, in certain circumstances we may obtain some personal information about other individuals. For example for:

- A beneficiary you nominate for your product.
- A family member or friend you authorise to make enquiries about your product on your behalf.
- Parents and/or grandparents of a minor for whom a product has been taken out.
- Potential beneficiaries, in the event of a death, so we can determine who we should pay any funds to.
- Any legal personal representatives (where applicable).
- An ex-spouse in relation to a pension sharing order or pension attachment order.
- The trustee where death benefits are paid to a trust.
- Anyone holding a lasting power of attorney or similar.

We'll process their personal information in accordance with this Privacy notice.

Our data security policies mean that we hold all personal information securely and limit access to those who need to see it in line with our obligations under data protection law. We apply extra security to more sensitive personal information, such as medical details, which are required to administer certain products, such as our Protection products.

Details of the companies that provide products and services within the Aegon UK Group are shown below:

- Cofunds Limited: Level 26 The Leadenhall Building, 122 Leadenhall Street, London EC3V 4AB. Company number – 03965289
- Scottish Equitable PLC: Aegon Lochside Crescent, Edinburgh Park, Edinburgh EH12 9SE. Company number – SC144517
- Aegon Investment Solutions Ltd: Aegon Lochside Crescent, Edinburgh Park, Edinburgh EH12 9SE. Company number – SC394519

Contact details

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

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

Email: **dataprotection@aegon.co.uk**

If you're contacting us by email please remember not to send any personal, financial or banking information because email isn't a secure method of communication. If you decide to send information in this way, you're doing so at your own risk as there's no guarantee that any email sent by you to us will be received or remain private during transmission.

How we obtain the personal information

You or someone representing you, for example, your intermediary or financial adviser, will provide us with personal information about you. Where you are a member of a workplace pension scheme, we'll receive information about you from your employer. Where you are a member of a Trust based pension scheme, we'll receive information about you from the trustees of the pension scheme.

We may obtain information about you via application forms (including claim forms), both paper-based and online, or by phone, email, social media tools or otherwise.

You can find additional information on the more common ways we capture your personal information below:

Method	Description
Application and claim forms from you or your representative	We obtain personal information about you through our application/claim forms (both paper and completed online) where we ask for specific information to be provided so we can process your application/claim. This may include copies of any identification documentation (for example, driving licence or passport) you need to provide as part of the application/claim process. For our protection products, there may be occasions where we'll use information that was previously provided to us, for example, information that was disclosed in an earlier application, in conjunction with details provided in any new application. This will include any application that didn't result in a policy becoming active, but only where the information is held in line with our retention schedule. Using this information allows us to identify any potential mis-representation or discrepancy, along with helping to improve the customer experience.
Phone calls from you or your representative	When you (or your representative) call us, we'll ask for some personal information to enable us to identify you or the authorised representative, and capture information relating to the query or otherwise during the call. Other personal information may then be disclosed to us during the call. In most circumstances, the call will be recorded and held for 16 years in line with our retention schedule.
Electronically from your employer or existing scheme trustees	Where you are part of your employer's pension scheme, we'll obtain personal information about you from either your employer or the nominated scheme trustees to administer the scheme appropriately. This information is usually sent to us electronically.
Publicly available information	On some occasions, we may collect and use personal information about you that has been made publicly available, for example, in public social media sites. This type of information would be used in limited circumstances and as part of our claims investigation and decision making process.
Competitions or surveys	If you enter any competitions or take part in a survey, we'll need to capture some minimal personal information from you.

We may also obtain personal information from third party sources, such as:

- Service providers who help us to maintain the integrity and accuracy of our data, for example:
  - Providing us with updated address details for customers who've moved house and not informed us.
  - Detecting individuals who are deceased.
- Credit management companies who are acting on your instruction.
- Credit reference agencies.
- Healthcare providers and medical practitioners.
- Comparison websites that you've used to look into specific products that we sell.
- Other pension providers to facilitate transfers to or from us.
- Parties you've instructed to act on your behalf, for example, your representative, a family member or solicitor who is acting under a power of attorney, as well as accountants, lawyers and other professional service firms that you've given authority to.
- Regulators, such as the Information Commissioners Office (ICO), the Pensions Regulator (TPR), the Financial Conduct Authority (FCA) and the Financial Ombudsman Service (FOS).
- Private investigators (only used in rare circumstances for certain claims).
- Financial crime detection agencies, sanction lists and databases.
- Government agencies and bodies, such as the courts, the Department for Work and Pensions (DWP), HM Revenue & Customs (HMRC) and the police.
- Where Aegon acquire another organisation that holds your information.

The types of information that we collect and hold about you

The type of information we process about you will depend on the type of product, service or interaction you have with us, and without it, it's unlikely we could provide you with a product or service. The type of information processed could include the following - This list is non-exhaustive:

Category	Data type
Contact information	Home address, email address, telephone (home and mobile) number
General	Name, nationality, date of birth, marital/relationship status, policy/plan number
Financial	Bank account/card details, transactional/contribution information, tax details, fund values
Government identifiers	Passport, ID card or Drivers Licence number (including copies of these for identification purposes), National Insurance number
Physical characteristics	Gender, health data (both physical & mental), racial or ethnic origin, sexual preference/life, religion or philosophical beliefs We don't necessarily request all these data types – some may become available to us indirectly via other means, for example, through information provided on an application form, or captured during a phone call.
Authentication	Login credentials

Category	Data type
Vulnerability	Details regarding life events (including aspects such as health, personal circumstances etc.) that will help us to identify if you are someone who may be classed as vulnerable so we can best meet your needs
Crime, fraud and sanctions	Criminal offences/convictions (including alleged), information received via sanction lists and fraud databases
Employment	Job title, salary, length of service
Marketing (including surveys and competitions)	Marketing preferences (opt in or out), responses to surveys including those relating to your customer experience, responses to competitions
Device information	IP address, location data, unique device ID

Sensitive personal information

There will be occasions where we'll ask for (or receive) sensitive personal information, also known as special categories of personal data. This consists of information relating to:

- Health (for example, a medical condition)
- Racial or ethnic origin
- Religious or philosophical beliefs
- Genetic or biometric data
- Sex life or sexual orientation
- Political opinions
- Trade union membership
- Criminal convictions and offences

An example of the type of situation where we'll capture sensitive personal information about you is if you take out a Protection product with us, for example, life or critical illness cover. As part of that process, we are required to capture some health information so we can assess and identify applications that may have an increased risk and where appropriate, determine the rate of premium or whether special terms are required.

The most common types of sensitive personal information we process are:

- Health information: this could include information contained within medical reports, test results, details of your physical and/or mental health condition (previous and existing), medication prescribed to you, medical diagnoses, details of any treatment plans, personal behaviours, such as alcohol consumption and smoking (where applicable).
- Criminal information: for the purposes of detecting or preventing financial crime, we may obtain information relating to criminal activity such as suspected fraud and criminal convictions.

We may also process other types of sensitive personal information simply because it can be derived from other information provided to us.

We apply extra security around this type of information as we appreciate that due to its very nature, it would likely cause significant harm or distress if mistreated.

How we use personal information

We have listed below the ways in which we will use the personal information that we collect:

Category	Data type
General & ongoing administration	▪ Administer your product from inception through to settlement/transfer/claim. ▪ Communicate with you and other parties. ▪ Manage third party relationships, for example, with intermediaries. ▪ Collect and apply payments. ▪ Produce and issue all necessary and regulatory documentation, for example, annual statements, policy documents etc. ▪ Facilitate settlements and claims, including transfers to other providers. ▪ Make any corrections/updates to personal information where required – for example, change of name or address. ▪ Manage complaints and feedback. ▪ Manage and respond to questions. ▪ Improve our products and services, provide staff training and maintain information security, including recording and monitoring of telephone calls. ▪ Manage our business operations, including conducting internal audits and reviews, financial analysis and producing management information. ▪ Testing of our IT systems, however if we do this, all personal information will be anonymised.
Regulatory	▪ Detect, prevent and investigate fraud and other financial crime activities by conducting anti-money laundering, fraud and sanction checks. ▪ To verify your identity (including bank details) and make decisions regarding the ongoing administration of your plan. ▪ Comply with all of our regulatory, legal and professional requirements, including co-operating fully with regulatory bodies, such as the FCA, PRA, ICO, the Pensions Regulator, and other government bodies. ▪ Help us to identify vulnerable customers, to enable us to better meet their needs and meet our regulatory responsibilities as to how we treat these individuals. ▪ Manage any requests where an individual chooses to exercise any of their rights.

Category	Data type
Marketing, profiling and data analysis	▪ Production and issuing of marketing materials, including running promotions but only where you have consented to this or where we are giving you information regarding similar products or services and you have not opted out of receiving such marketing. See 'Marketing consent and updating your preferences' for more information. ▪ Conduct customer insight, market research and focus groups, including campaign planning, creating promotional materials, gathering customer feedback and customer surveys to help us to improve the customer experience. Where we contact you for such a purpose, you're under no obligation to participate ▪ Conduct profiling and data analysis.
Other (ad-hoc)	▪ If we sell or buy any business or assets, we may disclose your personal information to the prospective seller or buyer to facilitate the continuity of service to you.

Please see additional information below on some of the uses.

Profiling and data analysis

We may use some of your data to conduct profiling and data analysis to build, train and audit models and algorithms that help us to:

- Understand our customers better to enable us to develop products and services that most appropriately meet their needs.
- Ensure we present the most appropriate content to customers.
- Identify instances where customers may require additional support.

We use various data types to conduct profiling and analysis and with all activities involving your information, we'll only do this where the law allows us to.

Our analysis isn't used to make any automated decisions about you directly but combined with data relating to other customers etc to enable us to make improvements to our processes and services.

Marketing consent and updating your preferences

Where you have consented or where it relates to similar products or services and you have not opted out of receiving such communications, we may use the information we've collected about you to send you marketing offers and news about our products and services using various channels such as mail, phone, email and SMS.

You can remove your consent or update your preferences at any time by logging into your secure online accounts and updating your profile, or you can write to or send an email to our Data Protection Officer.

We won't sell your personal information to other organisations for a marketing purpose.

We aim to limit the marketing materials that we send to you and will only send you offers or promotions that we believe you may be interested in.

Even where you opt out of marketing, we'll still send you servicing communications that are necessary for the management of your product and documentation relating to your product of which we have a legal duty to provide to you. You may also see generic advertising displayed on our website.

Email Tracking and Engagement Metrics

We use tracking technologies in our marketing emails to monitor email deliverability and engagement metrics, such as bounces, unsubscribes, opens, and clicks. This helps us to ensure that our communications are effective and relevant to our customers.

How we use email tracking data:

- Deliverability: To verify that emails are delivered to the correct addresses and to identify any issues with email delivery.
- Engagement: To understand how recipients interact with our emails, including whether they open the emails and click on links within them. This information helps us to improve our communications and tailor them to better meet the needs of our customers.
- Optimisation: To optimise our email content and strategy based on engagement metrics, ensuring that we provide valuable and engaging information to our customers.

You have the right to object to the use of tracking technologies in our emails. You can opt out of marketing communications at any time by using the unsubscribe link provided in our emails, this will mean you are unsubscribed from the promotional emails, but you will still receive servicing.

Cookies and similar technologies

We may use cookies and other similar tracking technologies on our websites, emails and apps.

Social media platforms

Any information users share with us on social media, for example, where you send us a private message, will be managed in line with the policies and procedures detailed in our **guidelines** (www.aegon.co.uk/utilities/privacy#/content/dam/auk/assets/publication/marketing-support/social-media-participation-guidelines.pdf).

Our lawful bases for using personal information

Data privacy laws state that we can only process personal information if it is lawful to do so. For the processing to be lawful, we must have a suitable lawful basis.

This section details our lawful bases for the various uses of both personal information and sensitive personal information.

Personal information

Depending on the specific purpose, we rely on one or more of the following lawful basis:

- To facilitate our fulfilment of a contract we have with you.
- In order to comply with a legal obligation on us.
- We have your consent.
- Where it's in Aegon's legitimate interests.

Legitimate interests

Where we have a business reason for using personal information in a certain way, this is known as being in our 'legitimate interests'. If we seek to rely on legitimate interests, we are required by law to conduct a balancing test to make sure that our interests don't override your rights and freedoms.

The outcome of this test determines whether we can rely on legitimate interests as our lawful basis and use the personal information for certain purposes as set out in this privacy notice. If the balance isn't met, we can't process your data in the way we had proposed.

Where we do rely on legitimate interests, it's because we believe our interests will be to the wider benefit of our customers and will normally relate to at least one of the following purposes:

- To assess, develop and improve our products and services.
- To enable us to understand our customers' needs.

- To help us to improve our customer engagement.
- To make sure we're treating our customers fairly.
- To ensure the integrity and functionality of our IT systems.
- To help keep our records up to date.
- To make sure we're efficient in how we fulfil our legal and contractual obligations.

Lawful basis for our processing of personal information

Purpose	Facilitate a contract	Legal obligation	Consent*	Legitimate interests
Administer your product from inception through to settlement/transfer/claim	✔	✔		
Communicate with you and other parties	✔	✔		✔
Manage third party relationships	✔			✔
Collect and apply payments	✔	✔		
Produce and issue all necessary and regulatory documentation	✔	✔		
Facilitate settlements and claims, including transfers to other providers	✔	✔		
Make any corrections/updates to personal information where required	✔	✔		
Manage complaints and feedback	✔	✔		
Manage and respond to questions	✔	✔		
Improve our products and services, including training of our staff, maintaining information security, including recording and monitoring of telephone calls		✔		✔
Manage our business operations		✔		✔
Testing of our IT systems				✔
Detect, prevent and investigate fraud and other financial crime activities	✔	✔		✔
Comply with all of our regulatory, legal and professional requirements		✔		
Help us to identify vulnerable customers		✔	✔	
Manage any requests where an individual chooses to exercise any of their rights		✔		

Purpose	Facilitate a contract	Legal obligation	Consent*	Legitimate interests
Production and issuing of marketing materials			✔	✔
Conduct customer insight, through market research, surveys and focus groups				✔
Profiling and data analysis				✔
Buy, sell, transfer or dispose of any of our business				✔
Email Tracking and Engagement Metrics				✔

* Where we rely on consent for specific processing and this isn't given, it means we are unable to use your data for this specific purpose. The consequences of this may mean that we are unable to record certain data about you which could help to tailor our service to your specific needs, or you could miss out on receiving marketing communications from us which may be of interest to you.

As mentioned previously, there will be occasions where we'll hold and process information which is defined as 'sensitive' or 'special'. Data privacy laws only allow us to use this type of information if we can rely on a further lawful basis, in addition to the one's shown above.

Depending on the specific purpose, we rely on one of the following lawful bases:

- For reasons of substantial public interest which includes insurance purposes comprising:
  - The ability to provide insurance – for example, using health information to be able to provide you with a Protection product.
  - The ability to detect and investigate fraudulent claims – for example, using criminal records data to help to prevent and detect unlawful acts.
  - Efficient administration and payment of insurance claims – for example, reviewing details of health conditions contained in medical reports to fully review and assess any claims.
- For the establishment, exercise or defence of legal claims – for example, using health or criminal records as required to establish, exercise or defend legal claims.
- The information has been made public by you – for example, when investigating an insurance claim, information that has been made public by you in social media sites etc could be taken into consideration as part of our assessment, or
- it's necessary to protect the vital interests of you or another party – for example, where an individual is either physically or legally incapable of giving consent.

Lawful basis for our processing of sensitive personal information

As mentioned previously, there will be occasions where we'll hold and process information which is defined as 'sensitive' or 'special'. Data privacy laws only allow us to use this type of information if we can rely on a further lawful basis, in addition to the one's shown above.

Depending on the specific purpose, we rely on one of the following lawful bases:

- For reasons of substantial public interest which includes insurance purposes comprising:
  - The ability to provide insurance for example, using health information to be able to provide you with a Protection product.

- The ability to detect and investigate fraudulent claims for example, using criminal records data to help to prevent and detect unlawful acts.
- Efficient administration and payment of insurance claims for example, reviewing details of health conditions contained in medical reports to fully review and assess any claims.

- For the establishment, exercise or defence of legal claims for example, using health or criminal records as required to establish, exercise or defend legal claims.
- The information has been made public by you for example, when investigating an insurance claim, information that has been made public by you in social media sites etc could be taken into consideration as part of our assessment.
- It's necessary to protect the vital interests of you or another party for example, where an individual is either physically or legally incapable of giving consent.

Sharing your personal information

Our service providers

We'll share personal information with selected service providers that carry out certain functions on our behalf. These include companies that provide services such as:

- Administration of our Protection and Traditional products.
- Technology services, including IT administration and support, software vendors, testing and production support, platform providers.
- Management of both inbound and outbound communications and scanning of correspondence.
- Providers of marketing, research or advertising services.
- Banking and payroll services.
- Tracing of customers who we've lost contact with, identifying customers who have deceased etc.
- Credit reference agencies for conducting verification/identity checks and follow-up biometric checks where necessary – see below for more details.

For those organisations that are carrying out services on our behalf, we'll only share information where we have a lawful basis for doing so, as described above. We'll only share with them the appropriate level of personal information necessary to enable them to carry out the service. We contractually require all our service providers:

- To keep the information safe and protected at all times, and
- To only act on our explicit instructions and not use the data for their own purposes, unless it has been suitably anonymised so it's no longer personal information.

Credit Reference Agencies

Credit reference agencies may be used to support verification checks. These bureaus (such as Experian, Equifax or TransUnion) may collect information about consumers and businesses from various sources and build databases that hold all of this data. Consumers have certain rights that they can seek to exercise in relation to the personal data held by credit reference agencies.

When an organisation carries out a search of someone's information, they may record details of that search. This is known as a search footprint. This may be recorded by the bureaus listed below.

A link to each credit reference agency information notice, also known as a 'CRAIN', can be found below:

Experian (www.experian.co.uk/legal/crain/)

Equifax (www.equifax.co.uk/crain)

TransUnion (www.transunion.co.uk/legal/privacy-centre/pc-credit-reference)

Other parties we may share data with

It's often necessary for us to share personal information with other third parties where we have a lawful basis to do so, such as:

- Regulatory bodies such as the Information Commissioners Office (ICO), Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA), HMRC, Financial Ombudsman Service (FOS) and the Pensions Regulator.
- Intermediaries and financial advisers who are acting on you or your employers behalf.
- Your employer (this could be both past and present) and any party that provides services to your employer relating to the governance, administration and/or evaluation of their pension scheme, including providing advice to their members. Information, such as statistics, may be provided to your employer regarding the scheme's efficiency, for example, to evaluate pension savings.
- Trustees or administrators of a trust or pension scheme to facilitate the administration of the trust/scheme.
- Other parts of the Aegon Group.
- Organisations such as credit management companies, solicitors, accountants etc who are acting on your behalf.
- Sanction-checking providers, financial crime detection agencies, financial services organisations and other parties who assist with fraud investigations and/or maintain fraud detection databases. Please refer to Financial Crime Prevention for more information.
- Financial or Pensions Ombudsman, where you've asked them to investigate a matter with us. This disclosure would normally be based on your consent to share the necessary data with them.
- Our reinsurers who provide reinsurance services in respect of our Protection business.
- The investment funds into which your assets are invested and the managers of those funds.
- Other pension providers, for example, in respect of a transfer to or from us.
- Government agencies, such as the police, courts and Department for Work & Pensions (DWP), who may request information relating to you – we'll release data if there's a lawful reason to do so.
- General practitioners and other medical professionals in relation to a product you have taken out with us. For example, we may reach out to them to clarify or expand on answers you've given in a claim form, or information is required for the purposes of arranging and underwriting certain products.

Additional data sharing obligations

Except for the 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.
- When protecting your interests or the interests of others 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.
- If we sell or buy any business or assets, in which case we may disclose your personal information to the prospective seller or buyer.

Or

- If we, or substantially all of our assets are acquired by a third party, we may disclose your personal information to that third party in connection with the acquisition.

Financial crime prevention

We may disclose your information to credit, fraud and financial crime prevention agencies to enable us to verify your identity (including bank details) and make decisions regarding the ongoing administration of your plan. This

will be undertaken during the application or enrolment process and at various stages of your relationship with us to enable us to fulfil our statutory and legal obligations which require us to ensure our customer records are up to date and to manage any potential fraud risk. Our enquiries or searches may be recorded and these agencies may supply us with financial and/or other personal information.

To protect providers like ourselves and, ultimately, customers and customers' payments against fraudulent claims and crimes such as money laundering, tax evasion and terrorist financing, we and other providers may use information exchange registers to share information. When we're dealing with application's we may search these registers.

If a claim is made under your plan, information about you (including details provided on the application and claim form) will be put on the registers so that other insurers can see them if necessary.

If false or inaccurate information is provided and fraud is identified, details will be passed to fraud prevention agencies. Law enforcement agencies may access and use this information. We and other organisations may also access and use this information to prevent fraud, money laundering, tax evasion and terrorist financing, for example, when:

- Recovering debt.
- Checking details on proposals and claims for all types of insurance.

Please contact the Data Protection Officer if you'd like to receive details of the agencies used by Aegon UK.

We and other organisations may access and use the information recorded by credit, fraud, and financial crime agencies from other countries.

Automated decision making

Where you applied for one of our Protection products, for example, critical illness cover, we used an automated decision-making tool during the underwriting process. Rules were built into our underwriting tool which either generated an automated decision or referred to one of our underwriters.

Retention

We keep personal information for as long as is reasonably required for the purposes in which it was collected. In most circumstances, we'll keep your personal information for the lifetime of your product and up to 16 years after your relationship with us ends, for example, you settle your benefits. Under certain circumstances, we may have to retain your personal information for longer. This is to make sure that we meet our legal, regulatory and accounting needs as set out by regulatory bodies such as the FCA and others.

In some limited circumstances, we're required to keep some specific information for longer, for example, pension transfer information. We'll also retain files if we have reason to believe there's the possibility of litigation.

We have in place and maintain a retention schedule and regularly review our obligations to make sure we don't keep personal information longer than we're legally obliged to.

Your rights

You have several rights under data protection laws – you'll find details of each of these below.

If you chose to exercise any of your rights with regards to your personal information, to make sure that we're dealing with you, we may ask for evidence of identity. Where you have authorised a third party to act on your behalf, we'll conduct the necessary checks to make sure the appropriate authorisations have been received. This is to make sure that we only disclose information to the correct and, where applicable, authorised individual or organisation.

In line with our data protection obligations, we aim to respond to all valid requests relating to your personal information within one month. There may be some occasions where it will take us longer, for example, if the request is

exceptionally complex. However, in these situations, we'll let you know as soon as possible and provide details of when we'll be in a position to respond.

There may be occasions where we don't have to (fully) comply with a request. In these situations, we'll explain why we're unable to do this.

Right of access

The right to request a copy of the personal information we hold about you, along with certain information relating to the processing of your personal information. 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.

Right of data portability

The right, in certain circumstances, to have personal information that you have provided directly to us about you, transferred securely to another service provider in electronic form. This right is only applicable where:

- the processing of your personal information is based either on your consent or in line with the performance of a contract with you, and
- the processing of your personal information is carried out by automated (for example, electronic) means.

Right of rectification

The right to have any inaccurate personal information we hold about you corrected.

Right of erasure ('Right to be forgotten')

The right to have any out-of-date personal information deleted once there's no legal requirement or business need for us to retain it. This isn't an absolute right as we may need to consider other legal and regulatory requirements which could result in us having to retain your personal information for a specific period of time.

Right to restrict processing

The right to restrict some processing, in limited circumstances, and where we don't have legitimate grounds for processing your personal information.

Right to object

The right to object to your personal information being used to send you marketing material. We'll only ever send you marketing communications where you have consented or where it relates to similar products or services and you have not opted out of receiving such communications. You can remove or add your consent at any time.

You can also object where you have grounds relating to your particular circumstances and we rely on 'legitimate interests' as our lawful basis for processing your personal information. However, where we believe we have compelling legitimate grounds, we'll continue to process it.

Automated decision making

The right to not be subject to a decision made solely using automated means, including profiling, where the outcome adversely or significantly impacts you. This right doesn't apply where it's:

- Necessary for the purposes of a contract between Aegon and you.
- Authorised by law.
- Based on your explicit consent.

Exercising your rights

To exercise any of these rights, please contact our Data Protection Officer.

Sending data outside of the UK and European Economic Area (EEA)

The personal information that we or those acting on our behalf process, may be transferred outside of the UK or EEA, in connection with the above uses of personal information.

Where any such transfer occurs, we take the necessary steps to make sure that your personal information is protected to the same

standard as if it were in the UK. This will include measures such as the adoption of contractual agreements with the other party to make sure that adequate safeguards are put in place.

For any transfers to another part of the Aegon group, these will be covered by an agreement which also obliges the other group member to make sure that adequate safeguards are put in place.

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 this, you can make a complaint 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 also raise a complaint with the Information Commissioner's Office, the UK's independent authority set up to enforce the Data Protection Regulations.

You can contact them at:

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Website: **ico.org.uk/global/contact-us/**

Phone: 0303 123 1113

Security

We're committed to making sure your information is protected and held securely in accordance with our obligations under data protection law. However, the internet isn't a secure medium and we can't accept responsibility for the security of an email during transmission or for non-delivery of an email.

There are a few simple steps you can take to protect your computer and internet connection – view our tips at www.aegon.co.uk/online-security-and-fraud-protection

We've put security policies, rules and technical measures in place to protect the personal information that we have under our control from:

- Unauthorised access.
- Improper use or disclosure.
- Unauthorised modification.
- Unlawful destruction or accidental loss.

All our employees and service providers who have access to personal information, are obliged to protect it and keep it confidential.

Links

This website may contain links to other websites. If you use the links to leave this website and visit a website operated by a third party, then we don't have any control over that website. We can't be held responsible for the protection and privacy of any information that you provide while visiting such websites..

Updates to this notice

We update our Privacy notice regularly to make sure it continues to reflect our business activities and use of personal information. You can find the date this was last updated at the beginning of this notice.

GEN06774 02/25