

Privacy Notice

All the Product Providers; Aviva, Canada Life, Just, Legal & General and Scottish Widows, that take part in the Retirement Health Form Service (referred to as “Product Providers” or “we” in this Privacy Notice (PN)) take their privacy obligations very seriously. Any personal information provided to them, as Data Controllers, by a policyholder, joint policyholder, employer policyholder, trustee, insured person, beneficiary, claimant or member (referred to as ‘you’ or ‘your’ in this PN), will be treated in accordance with current Data Protection legislation, and any successor legislation. This is a generic PN which explains how the Product Providers may use your personal information. Full details of how each Provider will use your data can be found on their websites:

Aviva - www.aviva.co.uk/legal/privacy-policy.html

Canada Life - www.canadalife.co.uk/data-protection-notice

Just - www.wearejust.co.uk/privacy-policy

Legal & General - www.legalandgeneral.com/privacy-policy

Scottish Widows - www.scottishwidows.co.uk/legal-information/legal-and-privacy/

What is personal information?

Personal information means any information about you which is personally identifiable, including your name, age, address, telephone number, email address, financial details, and any other information from which you can be identified. It will also include genetic and biometric data, location data and online identifiers which may identify you, such as your internet protocol (IP) address (the unique personal address which identifies your device on the internet) and mobile device IDs.

What do we collect?

The Product Providers will collect the following information about you and your dependants (this includes your authorised Power of Attorney) when you use their services or they may collect it indirectly from their business partners, such as financial intermediaries:

- Personal data: your name, date of birth, telephone number, address, email address, dependants, marital status, IP address and media access control (MAC) address.
- Sensitive/special categories of personal data: gender and other sensitive information such as information about your physical and mental health. They recognise that information about health is particularly sensitive information. Should consent be the legal basis of processing special categories of personal data, they will ask for consent to collect and use this information.
- Financial information: information that may relate to your financial circumstances (for example your pension values, income and existing investments), bank account details and details of product options you may consider.
- Technical Information: such as details on the devices and technology you use.
- Public Records: This includes open data such as the Electoral register, Land register or information that is openly available on the internet.
- Documentary data and national identifiers: Information that is stored on your passport, driving license, birth certificate, and National Insurance number.

As well as collecting personal information about you, they may also use personal information about other people, for example family members you wish to insure on a policy. If you are providing information about another person, the Product Providers expect you to ensure the other person knows you are doing so and are content with their information being provided to them. You might find it helpful to show them this PN and if they have any concerns to contact the relevant Product Provider(s) directly. If personal information is submitted about another person (for example spouse/partner), then by signing this form, you confirm that they have consented to providing their information for the information to be used and shared as set out in this notice.

How we use the information we collect

Product Providers on this form will use personal information collected from you and personal information about you obtained from other sources such as your financial intermediary in the following ways:

- To provide you with your required policy;
- To decide what terms, they can offer;
- To administer your policy;
- To support legitimate interests that they have as a business;
- To prevent, detect or investigate financial crime;
- To help them better understand their customers and improve customer engagement. This may include research; statistical analysis, profiling and customer analytics which allows them to make certain predictions and assumptions about your interests, and make correlations about their customers to improve their products;
- To meet any applicable legal or regulatory obligations: they need this to meet compliance requirements with their regulators (e.g. Financial Conduct Authority), to comply with law enforcement and to manage legal claims; and
- To carry out other activities that are in the public interest: for example, they may need to use personal information to carry out anti-money laundering checks.

Some of the information they collect as part of an application for a policy may be provided to them by a third party. This may include information Product Providers and their subsidiaries already hold about you and your dependant, including details from previous quotes and claims, information they obtain from publicly available records, their trusted third parties and from industry databases, including fraud prevention agencies and databases.

Legal basis for processing Personal Data

Where processing of data is necessary for entering into a contract with a Product Provider or for the performance of a contract which you (the data subject) are aware of the legal processing of Personal Data, this is based on Article 6.1(b) of the General Data Protection Regulation (GDPR).

Processing of Special Categories of Personal Data (for example health or medical data) is based on Article 9.2(g) of the GDPR in that processing is necessary for reasons of substantial public interest and conducted on the basis of applicable law where the only data processed will be that necessary for the aim specified in order to respect the Data Subject's rights and interests.

Who your Personal Information may be shared with

The personal information a Product Provider holds about you may be shared with the following recipients subject to security, contractual and transfer adequacy safeguards as appropriate:

- (a) their group affiliates (where they exist);
- (b) their agents;
- (c) their business partners/service providers who assist them in providing the services they offer;
- (d) doctors or any relevant medical professional; and
- (e) credit agencies (for the purpose of identification verification).

The following categories of agents, business partners and close affiliations assist them in the provision of ancillary services and they only use your personal information to the extent necessary to perform their functions:

- Providers for pricing/underwriting purposes: these Providers may share your personal information with their group companies for the same purpose;
- Service providers: for the provision of support services such as reinsurance, product administration, receiving and sending marketing communications, data analysis and validation, IT support services, archiving, auditing, business administration and other support services and tasks, from to time;
- Business partners who may have referred you to us: to provide them with relevant management information;
- Other companies in the event we undergo a re-organisation or are sold to a third party;
- Regulators and public authorities who have a legal right to request and process your personal information e.g. the FCA, HMRC and the DWP;
- Other subsidiary companies, where relevant, for management information purposes;
- In addition, a Product Provider may disclose your personal information if legally entitled or required to do so, for example, if required by law or by a court order or if they believe that such action is necessary to prevent fraud or cybercrime or to protect their website or the rights of individuals or their property or the personal safety of any person.

How long Product Providers will keep your Personal Information for

Product Providers maintain a retention policy to ensure they only keep personal information for as long as they reasonably need it for the purposes explained in this notice. They need to keep information for the period necessary to administer your insurance and deal with claims and queries on your policy. They may also need to keep information after their relationship with you has ended, for example, to ensure they have an accurate record in the event of any complaints or challenges, carry out relevant fraud checks, or where they are required to do so for legal, regulatory or tax purposes.

Anonymised personal information will not be considered as personal since no individual can be identified by that information. Product Providers may use anonymised personal information for further actuarial and business analysis, business research and reporting to help develop their products and services.

Transmission and Security of Personal Information

Product Providers have security measures in place to protect against the loss, misuse and alteration of personal information under their control as required by current Data Protection laws and, as of May 2018, the EU GDPR.

For example, Product Providers' security and privacy policies are periodically reviewed and enhanced as necessary and only authorised personnel have access to personal information. Whilst they cannot ensure or guarantee that loss, misuse or alteration of information will never occur, they will use all reasonable efforts to prevent it.

Data Transfer outside of the European Economic Area (EEA)

Given the global nature of some Product Providers' businesses, some will use third party suppliers and outsourced services (including Cloud-based services), which can require transfers of personal information outside of the EEA. In doing so, Product Providers will ensure that there are appropriate contractual arrangements in place and will choose only those organisations with strict controls via appropriate organisational and technical measures to protect your personal information.

Notification of Changes to Privacy Policy

Product Providers will reserve the right to amend or modify the Privacy Policy at any time and in response to any changes in applicable Data Protection and privacy legislation.

If Product Providers decide to change their Privacy Policy, they will post these changes on their websites so that you are aware of the information they collect and use it at all times.

If at any point Product Providers decide to use or disclose information they have collected, in a manner different from that stated at the time it was collected, they will notify you.

Individual rights under the General Data Protection Regulation

From 25th May 2018 individuals (Data Subjects) are provided with various rights including the right to be told what Personal Data is held by Product Providers and the right to request that any inaccuracies in respect of your Personal Data are corrected. Details of all individual rights are shown below:

- 1. The right to be informed** – you have the right to be informed how your Personal Data will be used. For example, this may be set out in a company's Privacy Notice.
- 2. The right of access** – you have the right to access your Personal Data and supplementary information. For example, you may wish to access your data to become aware of and verify the lawfulness of the processing.
- 3. The right to rectification** – you have the right to have your Personal Data rectified. For example, if you feel it is inaccurate or incomplete.
- 4. The right to erasure** – you have the right in specific circumstances to request the deletion or removal of Personal Data where there is no compelling reason for its continued processing. For example, your Personal Data was unlawfully processed.
- 5. The right to restrict processing** – you have the right to restrict the processing of your Personal Data in certain circumstances. For example, you wish to contest the accuracy of your Personal Data.
- 6. The right to data portability** – you have the right to obtain and reuse your Personal Data for your own purposes. For example, you may wish to move, copy or transfer Personal Data from one information technology environment to another in a safe and secure manner.
- 7. The right to object** – you have the right to object to your Personal Data being used for processing based on legitimate interests or for a task in the public interest. For example, you no longer want your Personal Data used for direct marketing.
- 8. Rights in relation to automated decision making and profiling** – you have the right to challenge decisions that are made using an automated approach including profiling. For example, you may want to request human intervention where you do not agree with an automated decision.

Contact Details:

Any enquiries relating to Data Protection issues should be sent to a Provider at the Data Protection address which can be found on page 18 of this form or from their website.

You also have the right to talk to the Information Commissioner's Office whose main role is to uphold information rights in the public interest.

Website: ico.org.uk/for-the-public

Email: casework@ico.org.uk

Phone: 0303 123 1113

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