

Retirement Privacy Policy

Last updated: 23 Aug 2023

1. Introduction

This Privacy Policy explains **how we use Personal Information** which we collect about individuals in relation to our retirement products and services.

We take the security of your Personal Information very seriously. We use a combination of technical, organisational and physical security measures to protect your Personal Information in line with our obligations under data protection law. Our employees receive training to help us comply with data protection law and safeguard your privacy.

This Privacy Policy is issued on behalf of the Aviva group companies within the United Kingdom. When we mention "Aviva", "we", "us" or "our", what we mean is the relevant company in the Aviva group that processes your Personal Information.

Each Aviva group company that processes your Personal Information is responsible for looking after it in accordance with this Privacy Policy. The Aviva group company that provides the product or service will be the main company responsible for your Personal Information, known as the controller. Please check the documentation that we provide to you for details of the specific Aviva company acting as controller of your Personal Information. If you are unsure, please **contact us**. We may share your Personal Information in accordance with this Privacy Policy with other companies in the Aviva group (including Wealthify Limited) with other companies in the Aviva group (including Wealthify Limited).

We have separate privacy notices for our different types of products, so if you have a number of Aviva products you may need to review more than one privacy notice. We may also supplement this Privacy Policy with additional privacy notices tailored to our specific relationships with you where this is useful to provide you with a full picture of how we collect and use your Personal Information. This Privacy Policy supplements – but doesn't override – them.

Most of the Personal Information we collect relates to the individual who is taking out a product (or individuals where it's taken out jointly). We may also ask for Personal Information about other individuals if we need it. For example:

- if you ask us to provide a product for other household or family members;
- if we ask you to provide health information about other family members where this is relevant to the risk we're covering;
- where you nominate an individual to receive payments upon your death; and
- where there are other people who are occupants at the property which is subject to a lifetime mortgage.

If you provide us with Personal Information about someone else including if you are an employer providing Personal Information about your employees or someone else, we'll assume that you have their permission, where required. We'll process their Personal Information according to this Privacy Policy so please encourage them to read it if they want to find out more.

2. Personal Information We Collect and How it is Used

Sources of Personal Information

We obtain Personal Information directly from you, including from application and claims forms that you complete, communications between us, your participation in promotions and market research, your use of our apps and websites and details of the devices you use to interact with our apps and websites. Where you are a beneficiary, we obtain Personal Information from the person who took out the product (e.g. your spouse) and where you are a member of an occupational or workplace pension scheme, we will obtain information from your employer (past and current) and the trustees of the pension.

We may also obtain Personal Information from third parties, including the following:

- Financial advisers, intermediaries, or one of our business partners, where you have purchased a product through one of these third parties;
- Comparison websites and other similar companies where you have used these companies to research our products;
- Other third parties involved in the relevant product or plan, including other product providers, financial advisers, trustees and banks;

- If you have an occupational or workplace pension scheme, your employer (past and current), which includes your employer's affiliated companies where those companies share a centralised pension administration function;
- Healthcare providers and medical practitioners;
- Your attorney acting under a power of attorney;
- Legal advisers, accountants, auditors and professional service firms who act on our or your behalf or on behalf of your employer (past and current);
- Service providers in relation to the relevant product or plan, including experts and in limited circumstances, private investigators;
- Aviva group companies who may provide information in relation to other products you or people you live with hold, previous claims, policies or quotes;
- Credit reference agencies;
- Financial crime detection agencies, databases and sanctions lists;
- Government agencies and regulatory bodies, including the police, the courts, the Office for National Statistics, the Department for Work and Pensions (DWP), Companies House and HM Revenue & Customs (HMRC);
- Regulators who regulate how we operate, including the Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA), Information Commissioner's Office (ICO), Pensions Regulator and Financial Ombudsman Service (FOS);
- Third parties who provide us with details of individuals who have expressed an interest in hearing about insurance products;
- Third parties that provide services in relation to your product, including property surveys and valuations
- Third parties that help us maintain the accuracy of our data e.g. by identifying individuals who are deceased, updating contact details for individuals who have moved;
- Other third party suppliers actuaries, auditors, legal advisers and other professional services firms and sanctions-checking service providers;
- Providers of marketing and advertising services;
- Data suppliers, e.g. Experian and **LexisNexis** (<https://risk.lexisnexis.com/group/processing-notice>) ;
- Publicly available sources, including the Office for National Statistics (e.g. census data) and other data made available under the Open Government Licence, internet searches, news articles, online marketplaces and social media sites, apps and networks (e.g. Twitter, Facebook and Instagram);
- Third parties in connection with any acquisition of a business by us.

Types of Personal Information collected

The Personal Information we hold and process will differ depending upon the retirement product or service that you have. It includes:

Information provided by you or third parties, including:

- General data – includes your name, date of birth, marital status, country of residence/citizenship and your relationships to other people, e.g. beneficiaries of a product or other occupiers of your home.
- Contact data – includes your address, telephone number and e-mail address.
- Identification data – includes government issued identification numbers, e.g. your national insurance number, passport number or driving licence number and other identifiers, e.g. usernames and social media identifiers.
- Appearance and behavioural data – includes your gender, age, hobbies, descriptive data, e.g. your height, images, demographic data and behavioural data, e.g. your lifestyle;
- Product data – includes information about quotes, policies, plans, schemes and any other information relevant to your product, including policy histories;
- Your home – how long you have lived at the property, property value, ownership status of your home, what proportion is owned by you, details about your existing lender;
- Fraud and sanctions related data – includes information obtained as a result of our investigations, e.g. carrying out checks of publicly available sources such as newspapers and social media sites and information obtained from checks of fraud databases and sanctions lists such as relationships/close associations with politically exposed persons;
- Employment-related data – includes your employment status, job title, salary and employment and history;
- Financial data – includes credit and payment card numbers (including updated card information provided by card issuers when changes are made), bank account details, payment information, tax information, details of income and assets, mortgages and pensions contributions and values;
- Vulnerability data – information about health, life events, resilience and capability that helps us identify if you might have additional support requirements in order that we can better meet your needs;
- Authentication data – includes account log-in information, passwords and memorable data for accessing your Aviva accounts;
- Telephone recordings and live chat transcripts – information obtained during recordings of telephone calls or live chats with our representatives and call centres;
- Marketing and communication preferences, promotion entries and customer feedback – includes marketing and communication preferences, information relating to promotions and prize draws, responses to surveys, complaints and details of your customer experience.

Information provided by third parties, including:

- Accurate contact data, e.g. where you have moved address, changed your telephone number or started using a new email address and not yet advised Aviva. This data may be used to ensure that we have a complete understanding of your product holding and to provide you with communications about your products. It will not be used for direct marketing purposes unless it was collected by the third party expressly for that purpose and always in accordance with data protection law;
- Data about the area you live in e.g:
 - your council tax band;

- average garden size;
- crime related data;
- census data;
- modelled data which predicts characteristics about people in your area, e.g. socio-economic groups as well as likely habits; and
- weather-related data.

Information collected from your devices, including:

Mobile device number, device type, operating system, browser, MAC address, IP address, location and account activity obtained through our use of cookies. You can find more about our use of cookies in our **Cookie Policy** (</services/about-our-business/products-and-services/cookie-policy/>) .

Information already held by Aviva, including:

- Data relating to other Aviva products or policies – e.g. savings and investments histories, policy and claim histories relating to other existing Aviva policies or products, or those you may have held in the past. , and contact details where you may have advised Aviva about a change on one product, but not another;
- Modelled data that has been developed by Aviva using data that it already holds.

Information inferred from your Personal Information, including:

- Appearance and behavioural data – includes your general interests, descriptive data and behavioural data e.g. to allow us to make certain predictions and assumptions about your interests, which allows us to personalise your experience with us;
- Estimated retirement income – includes your estimated retirement pot size, estimated retirement income and expected level of retirement lifestyle (based on the Pensions and Lifetime Savings Association (PLSA) Retirement Living Standards. The PLSA standards, based on independent research by Loughborough University, have been developed to help us to picture what kind of lifestyle we could have in retirement. The three levels are; Minimum, Moderate and Comfortable. More details can be found **here** (<https://www.retirementlivingstandards.org.uk/>) ;
- Vulnerability data – information about health, life events, resilience and capability that helps us identify if you might have additional support requirements in order that we can better meet your needs;
- Fraud and sanctions-related data – includes information obtained as a result of our investigations, e.g. carrying out checks of publicly available sources, such as newspapers and social media sites and checks of fraud databases and sanctions lists.

Children's data:

- We collect data about children in some circumstances, e.g. where they are beneficiaries of a product we provide.

Sensitive Personal Information

Sometimes we will request or receive Personal Information that is sensitive and we call this “Sensitive Personal Information”. This is information relating to your health, genetic or biometric data, sex life, sexual orientation, racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership. It also covers criminal offence data, including information about criminal activity, allegations (including those unproven), investigations, proceedings and penalties. For example, when you take out an annuity policy, we’ll need to ask for health information about you and anyone else to be covered under the policy. We know how sensitive this data is, so protecting it is a top priority. The types of Sensitive Personal Information we hold and process where relevant include:

- Health data – includes details of existing and previous physical or mental health conditions, health status, test results, medical diagnoses and treatment given, prescriptions and personal habits (e.g. smoking or consumption of alcohol);
- Criminal data – includes details of convictions e.g. in relation to detecting and preventing financial crime;
- Other sensitive data – in limited circumstances we may process other Sensitive Personal Information. For example, we may process sexual orientation data when we collect details of the gender of your spouse.

Uses of Personal Information

The main purposes for which we use Personal Information are to:

- **Communicate with you and other individuals;**
- **Make assessments and take decisions**, including whether to provide you with our products and services and on what terms. For further information, see [**Automated Decision Making**](#);
- **Process payments** when you purchase a product or service and any refunds;
- **Provide our products and services**, including administration, taking and making payments, making changes where requested or necessary, settlement and dispute resolution and the provision of our apps and other technologies, e.g. MyAviva;
- **Manage relationships with third parties**, e.g. financial advisers and service providers, who provide services either to you or to your employer (past and current);
- **Prevent, detect and investigate fraud and other crime**, including by carrying out fraud, sanctions and anti-money laundering checks. For further information see [**Fraud and Other Financial Crime**](#);
- **Improve our products and services, provide staff training and maintain information security**, including by recording and monitoring telephone and online calls and screen sharing sessions;
- **Provide marketing information and run promotions** in accordance with preferences you have expressed. For further information see the section on [**Marketing**](#);
- **Conduct customer insight analysis, market research and focus groups**, including customer segmentation, campaign planning, creating promotional materials, gathering customer feedback and customer satisfaction surveys;

- **Help us better understand our customers and improve our customer engagement**, including noting your interest in our website, understanding your customer journey, and use of profiled data (which is not actual information about you but predictions about you, e.g. assumptions about your interests based on the preferred leisure pursuits of households in your area). This allows us to make correlations about our customers to improve and promote our products and to suggest other products, services and information which may be relevant or of interest to customers;
- **Carry out data analysis**, including to ensure data accuracy and quality and for risk modelling and product and pricing refinement. For further information see [Profiling and Data Analysis](#);
- **Manage complaints**, including to allow us to respond to any current complaints, or challenges you or others might raise later, for internal training and monitoring purposes and to help us to improve our complaints handling processes. We may be obliged to forward details about your complaints, including your Personal Information, to the appropriate authorities, e.g. the relevant ombudsman;
- **Manage feedback and queries**, and handle requests to exercise data subject rights. For further information see [Data Rights](#);
- **Manage our business operations**, including by carrying out internal audits, quality assurance and training, financial analysis and accounting, producing management information and performing administrative activities in connection with the services we provide;
- **Manage commercial risk**, including by taking out and maintaining appropriate insurance and reinsurance;
- **Comply with applicable legal, regulatory and professional obligations**, including cooperating with regulatory bodies, e.g. the FCA, PRA, Pensions Regulator, ICO and government authorities, to comply with law enforcement and manage legal claims;
- **Identify and support customers requiring additional support**, to help us better meet your needs and to comply with regulatory guidance about how we meet your needs. Sometimes you or a third party may tell us that you have additional support requirements, and in other cases we may infer this from your Personal Information and our interactions with you;
- **Establish, enforce and defend our legal rights or those of third parties**, including enforcing our terms and conditions, pursuing available remedies and limiting our damages;
- **Carry out activities that are in the public interest**, e.g. we may need to use Personal Information to carry out anti-money laundering checks;
- **Buy, sell, transfer or dispose of any part of our business**;
- **Archiving, scientific or historical research or statistical purposes**

Lawful Bases for uses of Personal Information

We are committed to collecting and using Personal Information in accordance with applicable data protection laws. By law, we must have a legal justification, known as a lawful basis, in order to use

your Personal Information for the purposes described in this Privacy Policy. Depending upon the purpose, our lawful basis will be one of the following:

- Performance of a contract – to provide you with our products and services in accordance with their terms;
- Compliance with a legal obligation – to meet responsibilities we have to our regulators, tax officials, law enforcement, or other legal responsibilities;
- Legitimate interests – to operate and improve our products and services and keep people informed about our products and services or for any other purposes we identify as appropriate to our business needs, or those business needs of a third party;
- Consent – where we have obtained appropriate consents to collect or use your Personal Information for a particular purpose.

Where we rely on legitimate interests as our lawful basis, we are required to carry out a balancing test to ensure that our interests, or those of a third party, do not override the rights and freedoms that you have as an individual. The outcome of this balancing test will determine whether we can use your Personal Information for the purposes described in this Privacy Policy. Where we rely on the lawful basis of legitimate interests, the interests being relied upon will usually be:

- To further our business and commercial activities and objectives, or those of a third party, e.g. to provide our products and services and produce management information on our performance and the performance of third parties;
- To assist your employers (past and current) and third parties that are providing services to both you and your employer in respect of the administration, governance and evaluation of a pension scheme, including pension planning services for employees;
- To help us better understand our customers and improve our customer engagement including by carrying out marketing analytics and profiling, e.g. by making certain predictions and assumptions about your interests;
- To send you marketing information in accordance with your preferences, e.g. about other products and services we offer, and to administer promotions that you enter;
- To provide you with helpful information relating to your products and about useful tools for managing and engaging with your products, e.g. the MyAviva app. These are not marketing communications;
- To comply with our legal and regulatory obligations, guidelines, standards and codes of conduct, e.g. background checks or the prevention, detection and investigation of financial crime or fraud;
- To improve and develop our business, products and services, or those of a third party, e.g. to ensure the accuracy of customer data and to develop our pricing and risk methods and models;
- To retain records for a period of time in order to ensure we have appropriate records in place in respect of any future claims that may be made against us;
- To safeguard our business, shareholders, employees and customers, or those of a third party, e.g. maintaining the security of our IT network and information, enforcing claims, including debt collection;

- To facilitate the purchase, sale, transfer or disposal of any part of our business; and
- To analyse and assess competition in the market for our products services, e.g., by carrying out market research.

Our lawful bases for the use of Personal Information:

Purpose	Lawful Basis for Personal Information Processing
Communicating with you and others including complaints handling	Performance of a contract Compliance with a legal obligation Legitimate interests
Identifying customers requiring additional support	Compliance with a legal obligation Legitimate interests
Evaluating your application or renewal or to provide a quote	Performance of a contract Legitimate interests
Provision and administration of a product, including taking and making payment	Performance of a contract Compliance with a legal obligation Legitimate interests
Managing third party relationships e.g. financial advisers	Performance of a contract Legitimate interests
Claims assessment and management of claims	Performance of a contract Compliance with a legal obligation Legitimate interests
Financial or other crime, fraud and credit checks	Performance of a contract Compliance with a legal obligation Legitimate interests
Compliance with legal or regulatory obligations	Compliance with a legal obligation
Establish, enforce or defend legal rights	Compliance with a legal obligation Legitimate interests

Purpose	Lawful Basis for Personal Information Processing
Improving quality, training and security	Legitimate interests
Managing our business operations e.g. accounts, financial analysis, internal audit	Compliance with a legal obligation Legitimate interests
Data analysis (including modelling)	Legitimate interests
Applying for or claiming on our insurance	Performance of a contract Legitimate interests
Marketing and customer insight analysis, campaign planning etc	Legitimate interests Consent
Marketing in accordance with your preferences and administering promotions	Legitimate interests Consent
Buy, sell, transfer or dispose of our business	Compliance with a legal obligation Legitimate interests
Archiving, research or statistical purposes	Legitimate interests

We can only collect and use Sensitive Personal Information where we have an additional, specific lawful basis to process such information. We usually rely upon one of the following lawful bases where we process Sensitive Personal Information:

- Reasons of substantial public interest:
 - insurance purposes – including advising on, arranging, underwriting and administering contracts of insurance, administering claims under a contract of insurance and exercising rights, or complying with obligations that arise in connection with contracts of insurance;
 - occupational pensions – including processing health data which relates to an individual who is the parent, grandparent, great-grandparent or sibling of a member of an occupational pension scheme where it is necessary for determining eligibility for, or benefits payable under the scheme;
 - complying, or helping someone else comply with, a regulatory requirement relating to unlawful acts and dishonesty - including regulatory requirements to carry out money laundering checks;

- preventing or detecting unlawful acts – including disclosures to competent authorities;
- preventing fraud – including investigating alleged fraud;
- safeguarding the economic well-being of certain individuals – including where we identify additional support required by our customers;
- equality of opportunity or treatment – including where we need to keep under review the equality of treatment of customers with additional support needs.
- Necessary to establish, exercise or defend a legal claim – including where we are faced with legal proceedings, we bring legal proceedings ourselves or where we are investigating legal proceedings that a third party has brought against you;
- Necessary to protect your vital interests or those of another individual;
- Information has been clearly or obviously made public by you.

Our lawful bases for the use of Sensitive Personal Information:

Purpose	Lawful Basis for Sensitive Personal Information Processing
Communicating with you and others including complaints handling	Legal claims Necessary for insurance purposes Necessary for administering an occupational pension scheme Necessary for safeguarding economic well-being of certain individuals
Identifying customers requiring additional support	Necessary for safeguarding economic well-being of certain individuals Necessary for the equality of opportunity or treatment Explicit consent
Evaluating your application or renewal or to provide a quote	Legal claims Necessary for insurance purposes Necessary for administering an occupational pension scheme Explicit consent
Providing and administering a product, including taking and making payments	Necessary for insurance purposes Necessary for administering an occupational pension scheme

Purpose	Lawful Basis for Sensitive Personal Information Processing
Managing third party relationships, e.g. financial advisers	Necessary for insurance purposes Necessary for administering an occupational pension scheme
Claims assessment and management of claims	Necessary for insurance purposes Necessary for administering an occupational pension scheme Explicit consent
Identifying or investigating financial or other crime and fraud	Legal claims Regulatory requirement relating to unlawful acts or dishonesty Clearly or obviously made public by data subject Prevent or detect crime Prevent fraud Necessary for insurance purposes Necessary for administering an occupational pension scheme Necessary for safeguarding economic well-being of certain individuals
Compliance with legal or regulatory obligations	Legal claims Regulatory requirement relating to unlawful acts or dishonesty Necessary for insurance purposes Necessary for administering an occupational pension scheme
Establishing, enforcing or defending legal claims	Legal claims
Improving quality, training and security	Legal claims Explicit consent
Managing our business operations, e.g.	Legal claims

Purpose	Lawful Basis for Sensitive Personal Information Processing
accounts, financial analysis, internal audit	Explicit consent
Data analysis (including modelling)	Necessary for insurance purposes Necessary for administering an occupational pension scheme
Applying for or claiming on our insurance	Legal claims Necessary for insurance purposes
Buying, selling, transferring or disposing of our business	Necessary for insurance purposes Legal claims Explicit consent
Archiving, research or statistical analysis	Necessary for archiving, research or statistical analysis

Where we cannot rely on one of the above lawful bases to process your Sensitive Personal Information for a particular purpose, we will seek your explicit consent.

If you would like to know more about the lawful bases we rely upon, or how the lawful basis of legitimate interests applies to a particular purpose, you can **contact us**.

3. Who Personal Information is Shared With

In connection with the purposes set out above, we will sometimes share Personal Information with Aviva group companies and third parties, including:

- Financial advisers, intermediaries and business partners who help us arrange, manage and underwrite our products and who provide services;
- Other insurers and pension providers;
- Our insurers or reinsurers (either directly or through insurance brokers), who provide reinsurance services to us and each other in respect of risks underwritten by Aviva, or insurers who cover Aviva under our group insurance policies. We can supply on request

further details of the insurers and reinsurers we provide your Personal Information to and how this may be used. If you require further details, **contact us**;

- Your lifetime care or mortgage intermediary and other third parties providing services to them;
- Your employers (past and current), which includes any of your employers' affiliated companies where those companies share a centralised pension administration function, the trustees of the pension and third parties that are providing services to you or them in respect of the administration, governance and evaluation of a pension scheme, including pension planning services for employees. Information may be used to provide statistics to your employer in respect of the effectiveness of the pension scheme, e.g. to allow your employer to review calculations for employee pension savings and retirement income, and accurate contact details may be shared so that you can continue to receive information about your pension;
- Third parties who provide you with certain services;
- Third-party administrators who help us manage our products and services, including funding partners and other financial services organisations;
- Legal advisers, accountants, auditors, financial institutions and professional service firms who act on our or your behalf;
- Data analysts and providers of data services who support us with developing our products and prices and measuring the effectiveness of marketing;
- Third parties that help us maintain the accuracy of our data, e.g. by identifying individuals who are deceased, updating contact details for individuals who have moved;
- Financial crime detection agencies, sanctions-checking providers, financial services organisations and third parties who maintain fraud detection databases or provide assistance with investigation in cases of suspected fraud. For further information, see **Fraud and Other Financial Crime**;
- Regulators who regulate how we operate, including the FCA, PRA, FOS, HMRC, the Pensions Regulator, ICO and the Advertising Standards Authority;
- Government agencies and regulatory bodies including the police and courts;
- Industry bodies;
- Credit reference agencies;
- Service providers, including those who help operate our IT and back office systems, underwriting and claims processes and our information security controls;
- Third party payment service providers, including Adyen NV, who process card and other payments for us. For full details of how Adyen use your Personal Information when completing a transaction please refer to their **privacy policy (<https://www.adyen.com/policies-and-disclaimer/privacy-policy>)** ;
- Medical professionals, if we need to access health records or assessments for the purposes of arranging and underwriting certain products or facilitating and handling claims;
- Research agencies and providers of market research services, including customer feedback surveys;
- Providers of marketing and advertising services, including delivering and administering marketing, ensuring you receive marketing content that's relevant to you and in accordance

with your preferences and analysing marketing campaigns. These may include media agencies, fulfilment partners, social media and other online platforms and advertising technology companies. You can find further information about this in the section on **Marketing**;

- Third parties in connection with any sale, transfer or disposal of our business.

Some of the organisations we share information with may be located outside of the UK. For further information, please see the section on **International Data Transfers**.

4. Fraud and Other Financial Crime

We use your Personal Information to detect and prevent fraud and other financial crime such as market abuse including to meet our statutory and regulatory responsibilities in relation to fraud and financial crime.

If you're making an application or a claim, we may use profiling and other forms of automated processing to assess the probability that your application or claim may be fraudulent. This assessment may involve the use of Sensitive Personal Information.

We may also use your Personal Information including details of our interactions with you to help us detect fraud committed by brokers or financial advisers or to identify where you or a third party may be at risk of fraud or other financial crime.

To prevent, detect and investigate fraud and financial crime, we:

- check public registers (e.g. the electoral roll or registers of county court judgments, bankruptcy orders or repossessions);
- conduct online searches from websites, social media and other information sharing platforms;
- use databases managed by credit reference agencies, insurance industry bodies, fraud detection agencies and other reputable organisations; and
- share Personal Information and undertake searches with other third parties, including other insurers, fraud prevention agencies, law enforcement agencies, public bodies and our regulators (which include the FCA, PRA and ICO).

This will help us verify your identity, make decisions about providing you with our products and related services, e.g. paying claims and trace debtors or beneficiaries.

If you give us false or inaccurate information and we suspect fraud, we'll record this to prevent further fraud and money laundering and this may be shared with other parties.

We can supply on request further details of the agencies and databases we access or contribute to and how this information may be used. If you require further details **contact us**.

5. Automated Decision Making

We sometimes use automated processes to make decisions. These automated processes use data provided by you, other records we hold about you in our systems and data sourced from third parties to make predictions about the likelihood of certain events, including the likelihood that a claim will be made and its value, the likelihood a product will be purchased and the likelihood that a claim might be fraudulent. This helps us to determine eligibility for a policy, the terms of the policy and the price.

Where we make an automated decision using Personal Information which has a legal or substantially similar effect, you have certain rights in relation to that decision. In particular, you have the right to receive meaningful information about the logic involved in relation to the decision, the right to human intervention and the right to obtain an explanation of the decision and challenge it. For more information about this right and how to exercise it please see [**Data Rights**](#).

6. Profiling and Data Analysis

We use profiling and other data analysis to build, train and audit our insurance models and algorithms (including those used in our [**Automated Decision Making**](#)) and our machine-learning tools. The models, algorithms and tools we use help us do a number of things including:

- understanding our customers and potential customers better, e.g. how they feel about Aviva, what kind of content or products would be of most use and interest to them, whether they might be displaying characteristics meaning that they may require additional support from us; and
- predicting the likelihood of events arising to assess insurance risk, the likelihood a product will be purchased or to predict if a claim might be fraudulent.

We use a number of data items as described in this Privacy Policy for these purposes. Before we use any such data, we carry out a number of checks including ensuring there are no legal restrictions on using the data under data protection laws, the Equality Act 2010 or under FCA rules and we consider whether use of the data might cause outcomes that are unfairly or unlawfully biased. We then use statistical modelling techniques to assess the data to ensure that the data tells us something meaningful. From time to time, we may share your Personal Information with third

parties who provide us with new data which we will test to understand if such new data provides additional understanding.

We may also use profiling and data analysis for other reasons, e.g. to ensure data quality and accuracy and to help us improve our business.

The purpose of this analysis is not to make decisions about you directly, but your Personal Information, in combination with Personal Information relating to other customers, potential customers and/or data provided by third parties, will be used to conduct data analysis so that we can improve our processes, our products and services and the services being provided by third parties. We also use your Personal Information to check the way our models, algorithms and machine-learning tools work. The Personal Information you submitted to obtain a quote from us may be used for this analysis whether or not you decided to purchase the product.

Where possible, we pseudonymise the Personal Information in order to perform this analysis. This means that we remove information from which you can be directly identified, e.g. your name, and replace it with a pseudonym or unique identifier. We do this to maximise the security of your information.

We also use profiling in relation to marketing. For further information please see [**Marketing**](#).

7. Retention

We keep Personal Information for as long as is reasonably required for the purposes explained in this Privacy Policy. We also keep records – which may include Personal Information – to meet legal, regulatory, tax or accounting needs. For example, we are required to retain an accurate record of your dealings with us, so we can respond to any complaints or challenges you or others might raise later. We'll also retain files if we reasonably believe there is a prospect of litigation. The specific retention period for your Personal Information will depend on your relationship with us and the reasons we hold your Personal Information.

To support us in managing how long we hold your data and our record management, we maintain a data retention policy which includes clear guidelines on data retention and deletion.

If you would like more information about our data retention policy, please [**contact us**](#).

8. International Data Transfers

Sometimes we, or third parties acting on our behalf, may need to transfer Personal Information outside of the UK. We'll always take steps to ensure that any transfer of Personal Information outside the UK is carefully managed to protect your privacy rights and ensure that adequate safeguards are in place. This might include transfers to countries that the UK considers will provide adequate levels of data protection for your Personal Information (such as countries in the European Economic Area) or putting contractual obligations in place with the party we are sending information to. Transfers within the Aviva group will be covered by an agreement entered into by members of the Aviva group (an intra-group agreement) which contractually obliges each group company to ensure that your Personal Information receives an adequate and consistent level of protection wherever it is transferred within the group.

For more information about data transfers and the safeguards we have put in place, please **contact us.**

9. Marketing

We may use Personal Information to send you direct marketing communications about our products and services that we feel you'll be interested in. This may include marketing relating to products offered by other brands or companies within the Aviva group (such as quotemehappy, Wealthify and Succession Wealth) as well as communications about promotions and prize draws.

Marketing communications may be sent by email, post, SMS, telephone and push notification. You may also see display advertising on websites, mobile applications, social media, television or in online search results.

You have control over our use of your Personal Information in relation to marketing communications. You can:

- 'Opt out' of receiving direct marketing. When you register with us, request an online quote, or purchase a product or service you will be given the opportunity to opt out. In addition, our email, post, SMS and telephone marketing communications include information to help you manage your marketing preferences;
- Change your marketing preferences at any time by e-mailing us at **contactus@aviva.com** or writing to us at Aviva, Freepost, Mailing Exclusion Team, Unit 5, Wanlip Road Ind Est, Syston, Leicester, LE7 1PD. If you are registered for MyAviva you can change your marketing preferences at any time from within your account.

Please note that opting out of one type of marketing, e.g. by email or telephone, doesn't mean you will be opted out of all marketing. Bear this in mind when you manage your preferences. You can always contact us directly if you would like us to stop all forms of direct marketing.

We try to limit marketing and only send you offers and promotions that you might be interested in, based on Personal Information we have about you and profiling that we have carried out (further details can be found under the sub-heading 'Marketing profiles' below). We may use information provided by third parties to send you direct marketing and we may use your Personal Information to send other people direct marketing, e.g. people you live with.

Please remember that if you opt out of receiving marketing, we will still send you communications relating to your products. If you choose to opt out of tailored offers and advertising, you may still see generic advertising displayed online and in MyAviva, it just might not be as relevant to you.

Cookies and similar technologies

We rely on third-party advertising technology (such as the deployment of cookies or small text files on our website or pixels within emails) to collect information about you. This technology is used to optimise what you may see on our websites and deliver content when you are browsing elsewhere. We may also collect information about your use of other websites. We do this to provide you with advertising that we believe may be relevant for you, as well as to improve our own products and services.

For further information about cookies and other technologies we use on our website and how to manage cookies, please see our **Cookie Policy** (</services/about-our-business/products-and-services/cookie-policy/>) .

Social media and online platforms

We share Personal Information with media agencies and social media and other online platforms to help us target our online marketing. Social media and other online platforms may also use Personal Information they hold and combine it with Personal Information received from us to create target audiences. These are audiences that we think would be interested in our online advertising. This may involve social media and other online platforms building a 'lookalike' profile of the type of person we are trying to target and providing specific adverts to those people when they browse the internet or use social media.

If we use or share Personal Information with third parties in order to send you direct marketing, we will respect the marketing preferences you have set. We recommend you routinely review the privacy notices and preference settings that are available to you in MyAviva and any online platforms and smart devices you use as they will dictate how adverts and other messages are displayed and shared across those platforms.

Marketing profiles

We use automated processes to help us provide more personalised marketing of our products. To do this, our automated process creates a marketing profile for you using information such as:

- identification data;
- behavioural data (e.g. data relating to your use of our website);
- your gender and age;
- contact data;
- status data (e.g. number of children in household);

- product related data (e.g. policy identifiers, renewal dates);
- details of our interactions with you;
- device and vehicle-related data.

Our process analyses this data to determine the most relevant products, services, offers or benefits to offer you and to decide the appropriate time and channel for offering them to you.

Information obtained in relation to one product may be used in relation to marketing other products from the Aviva group.

We may also create profiles using your Personal Information together with information relating to other individuals, we use these profiles to decide what marketing may be of interest to individuals with similar characteristics to you.

Promotions and prize draws

We occasionally run promotions and prize draws for our customers and third parties. Our communications to you about these promotions before you enter them are marketing. If you opt out of receiving direct marketing, you will not receive communications about promotions and prize draws.

We may use your Personal Information to select you as a winner, inform you of promotion outcomes and send prizes to your nominated address. We may use third party fulfilment partners to assist us in administering promotions, including contacting you on our behalf. In accordance with the rules of the Advertising Standards Authority, we may publish or make publicly available information that indicates that a valid award has taken place. If we do this, only your surname, country and, if applicable, your winning entry, will be published. You have the right to object to this use of your Personal Information.

10. Data Rights

You have legal rights under data protection laws in relation to your Personal Information. Read below to learn more about each right you may have.

We may ask you for proof of identity when you make a request to exercise any of these rights. We do this to ensure we only disclose information to the right individual.

We aim to respond to all valid requests within one month. It may take us longer if the request is particularly complicated or you have made several requests. We'll always let you know if we think a response will take longer than one month. We may also ask you to provide more detail about what you want to receive or are concerned about.

We may not always be able to do what you have asked. This is because your rights will not always apply, e.g. if it would impact the duty of confidentiality we owe to others, or if the law allow us to

deal with the request in a different way. We will always explain to you how we are dealing with your request. In some circumstances (such as the right to erasure or withdrawal of consent), exercising a right might mean that we can no longer provide our product to you.

For further information about or to exercise any of your rights, please **contact us**. If you wish to make a subject access request, please **fill out this form** (</services/about-our-business/products-and-services/subject-access-request/>) .

Your rights are as follows:

Access to your Personal Information

You may ask us for a copy of your Personal Information together with specified details about how we use your information. This is commonly known as a 'subject access request'.

If you wish to make a subject access request, please **fill out this form** (</services/about-our-business/products-and-services/subject-access-request/>) or write to us using the details in **Contacting Aviva**.

If your request is made electronically, we will, where possible, respond to you electronically. Otherwise, we will normally respond in writing unless you request otherwise.

Rectification of your Personal Information

We do our best to ensure that your Personal Information is accurate and kept up to date. If you believe your information is inaccurate or incomplete, then please **contact us** to request that we amend or update it.

Erasing your Personal Information

You may ask us to erase your Personal Information, but this right only applies in certain circumstances, e.g. where:

- it is no longer necessary for us to use your Personal Information for the original purpose;
- our lawful basis for using your Personal Information is consent and you withdraw your consent; or
- our lawful basis is legitimate interests and there is no overriding legitimate interest to continue using your Personal Information if you object.

This isn't an absolute right and we have to balance your request against other factors such as legal or regulatory requirements, which may mean we cannot erase your Personal Information.

Restricting processing of your Personal Information

You may ask us to stop using your Personal Information in certain circumstances such as:

- where you have contacted us about the accuracy of your Personal Information and we are checking the accuracy;
- if you have objected to your Personal Information being used based on legitimate interests.

This isn't an absolute right and we may not be able to comply with your request.

Data portability

In some cases, you can ask us to transfer Personal Information that you have provided to us to another third party of your choice. This right only applies where:

- we have justified our use of your Personal Information based on your consent or the performance of a contract with you; and
 - our use of your Personal Information is by electronic means.
-

Right to object

You can object if you no longer wish to receive direct marketing from us.

You may also object where you have grounds relating to your particular situation and the lawful basis we rely on for using your Personal Information is our (or a third party's) legitimate interests. However, we may continue to use your Personal Information where there are compelling legitimate grounds to do so.

Automated decision making and profiling

You have the right not to be subject to a decision using your Personal Information which is based solely on automated processing (without human involvement) where that decision produces a legal effect or otherwise significantly affects you. This right does not apply if the decision is:

- necessary for the purposes of a contract between us and you;
- authorised by law (e.g. to prevent fraud); or
- based on your explicit consent.

You do however have a right to request human intervention, express your view and challenge the decision.

Withdrawing consent

In some circumstances we ask for your consent to use your Personal Information. You are free to withdraw your consent at any time.

If it is the case that we need your consent to provide you with a particular product and you wish to withdraw your consent, we may no longer be able to provide our product to you. Where that is the case, we will inform you before taking any action.

11. Contacting Aviva

If you have any questions about this Privacy Policy or how to exercise your rights, please contact our Data Protection Officer:

Write to: The Data Protection Team, Aviva, PO Box 7684, Pitheavlis, Perth PH2 1JR

Email us: DATAPRT@aviva.com

If you'd like to submit a subject access request, please **fill out this form** (</services/about-our-business/products-and-services/subject-access-request/>) or write to us at the above address.

If you're not happy with the way we're handling your Personal Information, you have a right to make a complaint with your local data protection supervisory authority at any time. In the UK this is the **Information Commissioner's Office (ICO)** (<https://ico.org.uk/>). We ask that you please attempt to resolve any issues with us before contacting the ICO.

12. Updates

This Privacy Policy is updated from time to time to take account of changes in our business activities, legal requirements and to make sure it's as transparent as possible, so please check back here for the current version. You can see when this Privacy Policy was last updated by checking at the top of this page.

Products, useful tools and information
