



Aviva Ireland Privacy Policy

Introduction

What Personal Information We Collect Use and Share When You Buy One of Our Products

General information

1. What we collect and from whom
2. Who we share information with
3. Working with Regulators and fraud prevention agencies
4. Using personal information to improve our products and services
5. Using personal information to create profiles and take automated decisions
6. Retaining personal information
7. Protecting personal information outside the EEA
8. Direct marketing and marketing preferences (for customers of Aviva Direct Insurance Ireland Ltd)
9. Working with credit reference agencies (for General Insurance Commercial Products only)

Specific product information

1. Motor and Home
2. Life, Critical Illness or Income Protection
3. Annuities
4. Pensions, Savings and Investments
5. Business insurance including motor and non-motor.

Legal Basis for Use of Information

Your Rights

1. To access personal information
2. To correct / erase personal information
3. To restrict how we use personal information
4. To object to how we use personal information
5. To ask us to transfer personal data to another organisation
6. To object to automated decisions
7. To obtain a copy of our safety measures
8. To withdraw consent

Contact Us

List of Aviva Group Companies

Introduction

At Aviva, we are committed to protecting the privacy of your data. This Policy tells you how we do this as well as informing you about your rights in relation to that data.

This Privacy Policy is issued on behalf of the Aviva Group companies operating within the Republic of Ireland. When we mention “Aviva”, “we”, “us” or “our” we are referring to the relevant company in the Aviva Group that [processes](#) your personal information. A list of these companies can be found at the end of this Policy.

The information in this Privacy Policy is important, so we have tried to make it very easy to navigate. You can read the document from start to finish or use the links to find the subject you want. Click on individual words shown in bold and underlined to see a brief definition of what they mean.

If you are an Aviva Ireland customer, we may provide you with separate privacy notices when we collect personal information from you, for example when you ask for a quote or apply for one of our products. Read those privacy notices with care, because they will tell you which Aviva company is responsible for managing your personal information and provide more specific information about how we will use your personal information in relation to that product. This Privacy Policy supplements, but does not override, those notices. This Privacy Policy is separate from and not intended to override the terms of any contract we may have with you or your rights under data protection laws.

Note: You don't have to provide us with any personal information, but if you don't provide the information we need we may not be able to proceed with your application or any claim you make. We will let you know what information is required to proceed with your application or any claim you make.

We may amend this Privacy Policy from time to time to keep it up to date with current legal requirements and the way we operate our business. Please regularly check these pages for the latest version.

What Personal Information We Collect, Use and Share When You Buy One of Our Products

1. What we Collect and from Whom

We are committed to collecting and using personal information in accordance with applicable data protection laws including GDPR and Irish Data Protection legislation.

Wherever we collect or use personal information, we will make sure we do this for a valid legal reason. This will be for at least one of the following purposes:

- to arrange, manage and administer or handle claims in accordance with the terms of one of our insurance, pension or investment products
- to meet responsibilities, we have to our regulators, tax authorities, law enforcement, or otherwise meet our legal responsibilities
- to operate and improve our portfolio of products and services and keep people informed about what we can offer
- for any other purposes where we have asked for and obtained consent to use personal information.

We explain more about these arrangements in other parts of this Privacy Policy and in the notices provided when we collect personal information. Please contact us if you would like to know more. Details of how to contact us are contained in this Policy

Information we collect can come from any of the following sources:

- You
- Information already held about you within the Aviva Group, including details from previous, policies of insurance and claims;
- from the intermediary, financial broker or other nominated representative;
- from recognised databases such as [Insurance link](#).
- from publicly available information including social media websites and online content, newspaper articles, television, radio and other media content, court judgements, public registers and specialist databases (for example Companies Registration Office, Vision-net, Oracle, Dow Jones, SoloCheck) and (only for purposes of verifying your identity) electoral register; and
- from an employer, other relevant insurance companies, trustees and pension providers, reinsurers and other insurance companies.

Type of information

The type of information we collect includes (not an exhaustive list):

Name, address (including Eircode), date of birth, policy numbers, contact details, PPS number (if required by legislation), employment details, gender, years of residency in Ireland or the UK, driving licence details, marketing preferences and renewal dates of policies with other insurers, bank and payment card details, records of payments and arrears, VAT and other relevant tax numbers, tax status (for some investment products) CCTV footage from our offices, membership status of any relevant bodies.

Further details of information we collect can be found under specific headings in this Policy and in the Data Protection Notice provided with your Product.

Sensitive information

For some products we may ask for health information or details of [past or pending offences](#) or other sensitive information about the person who is being insured, their family members and any other persons associated with the Policy. We recognise the sensitivity of collecting this information, so will only ask for it where we need it to arrange, manage or administer an insurance contract, handle claims, or prevent fraud. Where health data is requested, please do not send us any genetic test results. If we inadvertently come into possession of genetic data we will delete or mask it when possible and will not make use of it for any purpose.

Making a claim

If you are making a claim, we may use profiling and other forms of automated processing to assess if your claim may be fraudulent and we may use your sensitive personal information, to carry out this assessment. For example, we may use your past [unspent motoring convictions](#) for motoring insurance or we may use your medical history to carry out assessment for life insurance.

Fraud and Financial Crime

We will use your personal information to detect and prevent fraudulent practices and fight [financial crime](#) to meet our regulatory responsibilities.

Payment information

If you purchase a product directly from our website or other Aviva sales channel, we will ask for [payment](#) details. We need this information so we can process the payment associated with any product purchased.

Marketing, cookies and analytics

We collect information to help us improve our products and services and let people know about products and services that we believe will be of interest to them. This may be through a range of channels, including via email, online advertising or social media. We will always do this in accordance with marketing preferences provided. For a link to our cookie policy, please [click here](#).

Call Recording

We may record or monitor telephone calls in order to ensure accuracy in the recording of instructions communicated to us, to facilitate staff training, for the prevention of fraud, for management of complaints and to improve customer satisfaction.

Information about other individuals

Whilst most of the information we collect relates to the product holder, we do ask for information about other individuals if it is necessary to arrange, manage or administer an insurance contract, pension, or investment product, or handle claims. Common examples include:

- a policy holder asking us to provide insurance to other household or family members, or members of a group
- we may ask an insured to provide health information about other family members where this is relevant to the risk we are covering when we arrange a policy
- we may collect information about a number of individuals when we handle a claim, such as injured third parties.

If you provide information about another individual we expect you to ensure that they know you are doing so and are content with their information being provided to Aviva. We will process their personal information in accordance with this Privacy Policy so please encourage them to read this policy to find out more.

2. Who We Share Information With

If you purchase a product directly from our website or other Aviva sales channel, we will ask for payment details. We need this information so we can process the payment associated with any product purchased.

1. Other Aviva Group companies, agents, professional advisers acting for us (e.g. medical practitioners, lawyers, loss adjusters, private investigators) and third party service providers.
2. The intermediary/financial broker and at their request, third party service providers who provide services to the intermediary/financial broker (e.g. software providers who give brokers an overview of customer information across different insurance providers).
3. Your agents and other third parties relevant to you and/or the policy, including doctors and other relevant medical practitioners, employer, previous employers, other insurance companies, trustees, administrators and other pension providers.
4. If appropriate with regard to relevant legal/tax regulatory obligations and Revenue requirements: with regulatory bodies, law enforcement bodies, government departments including Central Bank of Ireland, Financial Services and Pensions Ombudsman, Revenue Commissioners/Inspector of Taxes, Gardaí, Criminal Assets Bureau, Data Protection Commission and Department of Employment Affairs and Social Protection.
5. With other insurers and financial services companies, public bodies, (either directly or using shared databases) and industry bodies such as Insurance Ireland.
6. With reinsurers who provide reinsurance services to Aviva. Reinsurers will use your data to decide whether to provide reinsurance cover, assess and deal with reinsurance claims and to meet legal

obligations. They will keep your data for the period necessary for these purposes and may need to disclose it to other companies within their group, their agents and third party service providers, law enforcement and regulatory bodies.

7. With Third Party claimants or their legal representatives in the course of dealing with the administration of a claim.

For particular products, e.g. motor insurance, we share information with specialist web based databases, State Agencies and regulatory authorities. Further details are provided in the Product sections of this Policy and in the Data Protection Notice you receive with your Product.

3. Working with Regulators and Fraud Prevention and Detection Agencies

We may use your personal information to allow us to detect and prevent fraudulent applications and claims and fight financial crime and meet our regulatory responsibilities. This may involve checking public registers e.g. the electoral roll or registers of court judgments, bankruptcy orders or repossessions, conducting online searches from websites, social media and other information sharing platforms for more details, our own and other Aviva Group company records and other reputable organisations. We also participate in industry databases, including [Insurance Link](#), for the purpose of sharing information among insurance companies as a check against non-disclosure. More information about [Insurance Link](#) can be found at www.inslink.ie. We will also check the validity of your No Claims Discount or previous insurance details with your previous insurer.

This will help us verify your identity, make decisions about providing you with our products and related services, and trace debtors or beneficiaries. We may also share your information and undertake searches with third party organisations such as the Garda Síochána, public bodies, fraud prevention agencies and our regulators (which include the Central Bank of Ireland, Financial Services Ombudsman, Data Protection Commissioner).

If you give us false or inaccurate information and we suspect fraud, we will record this to prevent further fraud and money laundering.

4. Using Personal Information to Improve our Products and Services

We collect information through cookies and other similar technologies (e.g. pixel tags or links) when you visit our websites or download and use one of our mobile apps. These tools are used by Aviva and our third party service providers to help improve our and their products and services, the functionality and performance of our websites and apps and support more effective advertising.

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 improve our own products and services, including the functionality and performance of our websites and Apps.

To learn more about these technologies and how you can use browser settings to manage your privacy controls, see our [Cookie Policy](#).

From time to time, we may contact you to seek your views on the products and service we offer. This contact may be made by a Third Party service provider using face to face, telephone, email or social media.

5. Using Personal Information to Create Profiles and make Automated Decisions

If you are applying for insurance, we may use tools to create profiles about you and, in some cases, use processes that apply these profiles to make fully automated decisions that may affect the services we provide to you.

In the context of arranging an insurance policy, these tools are often used to help assess individual risk or the impact your information might have on the cumulative risk of a group and calculate insurance premiums or to make a decision about whether to extend or renew cover. We may also apply automated decision making to [telematics data](#) to make decisions about renewal quotes or claims.

If you are making a claim, we may use profiling or other forms of automated processing to assess the probability that your claim may be fraudulent or suspect in some way.

Where sensitive personal information is relevant to the profiling, such as medical history for life insurance or past motoring convictions for motor insurance, your sensitive personal information may also be used in the profiling models.

Please note. You have certain rights in respect of automated decision making where that decision has significant effects on you, including where it produces a legal effect on you. Full details of your rights are can be found in the “Your Rights” section of this Policy.

Aviva Direct Insurance Ireland Ltd, in conjunction with a trusted research Partner carries out profiling of customer data to determine the likelihood that the customer will renew the policy or, in the case of prospective customers, buy a policy. This likelihood is referred to as the “propensity to lapse/buy”. The process involves assessing a number of factors including length of time with the company, claims experience, change in premium since last renewal, vehicle details etc. The results of the profiling are used solely to determine what type of contact is made with the customer at renewal or quote – e.g. a customer who is rated as likely to renew is contacted by telephone so that a conversation may be had to add value to the relationship. The results of this profiling work are not used in the calculation of a premium.

6. Retaining Personal Information

Our Policy is to only keep personal information for as long as is reasonably required for the purpose(s) for which it was collected. We do keep certain transactional records - which may include personal information - for more extended periods if we need to do this to meet legal, regulatory, tax or accounting needs. For instance, under the Consumer Protection Code, we are required to retain an accurate record of dealings with us for at least six years after your last interaction with us, so we can respond to any complaints or challenge you or others might raise later. We will also retain files if we reasonably believe there is a prospect of litigation.

We maintain a data retention policy which we apply to the records we hold. Where your personal information is no longer required we will ensure it is securely deleted, permanently obscured or put beyond use by our employees. In limited circumstances, this may not be technically possible and we will ensure that any such data will be held securely with access restricted to senior specialist employees. Generally we keep information for the periods set out in the table below:

Data	Retention Limit
Quote information (where a policy is not taken out)	15 months
Call Recordings	Training and Quality – up to 7 Years from the ending of the client/insurer relationship
Email Mailbox	No longer than is necessary
Individual Email	No longer than is necessary
Image Files	7 years after the end of the Client/Insurer relationship
Which may include personal and / or sensitive customer information	(Data is masked in line with the Data Retention policy for the type of data.)
Payment Files	Not Stored
Mainframe systems	7 years after the end of the Client/Insurer relationship
	Dependent on system
	Maximum 7 years
IT Back Up Files	Dependent on system
Disaster Recovery	As above
Paper documents held in locked storage	up to 7 Years from the ending of the client/insurer relationship

In some limited cases we may need to keep personal data longer than the above periods. Examples of these situations include long-running disputes and system back-ups required for disaster recovery.

We also retain certain limited details beyond the above time periods in order to validate and handle any claims we receive after the statute of limitations has expired (late claims) and any claims we receive where the claimant was not aware of the damage until a long time after it was caused (latent claims). In these circumstances we retain information such as the policyholder's name, the names of any named drivers, policy start and finish dates and cover details.

For late claims we will hold the data for a period of up to 25 years from the lapse or cancellation date of your policy or from the completion of a claim and for latent claims we will hold the data for up to 60 years from the lapse or cancellation date of your policy. In both cases, the data will only be used in the event that a new claim is made by or against you.

7. Protecting Information Outside the EEA

Some of the organisations we share information with may be located outside of the [European Economic Area \(EEA\)](#). We will always take steps to ensure that any transfer of information outside the EEA is carefully managed to protect your privacy rights:

Countries we transfer data to include India, Sri Lanka and Singapore but this is not an exhaustive list.

- 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 member to ensure that your personal information receives an adequate and consistent level of protection wherever it is transferred within the Group;
- where we transfer your data to non-Aviva Group members or other companies providing us with a service, we will obtain contractual commitments and assurances from them to protect your personal information. These assurances are well recognized certification schemes like Standard Contractual Clauses or the EU - U.S. Privacy Shield for the protection of personal information transferred from within the EU to the United States of America;

- we will only transfer personal information to countries which are recognised as providing an adequate level of legal protection or where we can be satisfied that alternative arrangements are in place to protect your privacy rights; and
- any requests for information we receive from law enforcement or regulators will be carefully validated before personal information is disclosed.

You have a right to ask us for more information about the safeguards we have put in place as mentioned above. To learn more, go to your rights section.

8. Direct Marketing and Marketing Preferences (for customers of Aviva Direct Insurance Ltd only)

If you are a customer of Aviva Direct Insurance Ireland Ltd, we may use personal information to send [direct marketing](#) communications about our insurance products and our related services where we believe this will be of interest. If we send this information in the form of email, post, SMS, telephone, mobile App or targeted online advertisements, we will only do so if you have provided us with consent.

- we take steps to limit [direct marketing](#) to a reasonable and proportionate level, and to send you communications which we believe may be of interest or relevance to you, based on the information we have about you.
- if we share use or share information with online sources, such as websites, social media and information sharing platforms to help tailor and improve our services or communicate with you effectively, we will respect any permissions you have set about how you would like your personal information to be used.

9. Working with Credit Reference Agencies – (applies only to General Insurance Commercial Policies)

To ensure we have the necessary facts to assess your insurance risk, verify your identity, help [prevent fraud](#) and provide you with our best premium and payment options, we may carry out a search for information relating to you with credit reference agencies. Credit reference agencies may keep a record of the searches we make with them. The only information we pass to credit reference agencies is information relating to your identity.

In addition to the general ways we [process](#) your personal information there is some specific information we need to use when you purchase a particular product. Please read the sections below to learn about what information we collect across our product range. If you want to skip to a product, click on one of these links.

1. Motor and Home

When you purchase a policy

- If you take out a motor policy with us, we will collect information about the driving licence number for each person included in the policy or proposal. We need this information to confirm the licence status of each driver and associated entitlement and relevant restriction information, Penalty Points and endorsement and conviction details. We do this by validating details against the [IDS Hub](#) and the [National Vehicle and Driver File \(NVDF\)](#). We will also add details of the policy to the [Motor Third Party Liability Database](#) maintained by the [Motor Insurers Bureau of Ireland \(MIBI\)](#). The MIBI may make this information available to authorised bodies such as the Department of Transport, Tourism and Sport, An Garda Síochána, and The Department of Justice and Equality. We will also provide details of the policy to other authorised bodies, as required by legislation from time to time, such as the Department of Finance.

- If you take out a home insurance policy with us we will collect information about your home and the persons residing within your property. We may refer to public registers and databases, such as Eircode and flood maps as well as information already held by Aviva where this will help us assess the risk associated with the policy;

If you make a claim

If you make a claim under any of our motor, home or travel insurance policies, we will need to collect information to help validate and administer the claim.

If you are making a claim following a motor accident, we will ask for details of the claim including, for accidents, information about those involved and any personal injury you or others may have suffered. We may also validate your claim by checking the licence details of the driver against the [IIDS Hub](#) or the [National Vehicle and Driver File \(NVFD\)](#). We may check your details against the [Insurance Link](#) database maintained by Insurance Ireland.

If you are making a claim under a home policy, we will ask you to confirm your identity and provide details of the claim.

2. Life Critical Illness or Income Protection

When you purchase a policy

If you request a quote for or take out a life critical illness or income protection insurance policy with us, we will collect information about the age, occupation, salary, benefits package, lifestyle, current state of health and any existing conditions of each person included in the policy or proposal. We may ask you to authorise a healthcare provider to supply relevant supporting information. We need this information to assess risk associated with the policy. We may also collect information about the family or personal history of the insured, where this is relevant to our risk assessment.

If you make a claim

If you are making a claim on a life insurance policy, we will ask you to confirm your identity, provide details of the policyholder and (if different) provide details of the insured, including details of their death so that we can assess the claim.

If you are making a claim under a critical illness or income protection policy, we will ask you to confirm your identity and provide details of your health condition. We may also ask you to authorise your healthcare provider to provide information to assist in assessing the claim.

3. Annuities

When you purchase an annuity

If you request information for or take out an annuity with us, we will collect information about your age, retirement age, occupation, lifestyle, current state of health, any existing health conditions, the value of your pension and your employment history in relation to your pension. We may ask you to authorise a healthcare provider to supply relevant supporting information. We need this information to assess risk associated with the product and to assess the appropriate price for you. We may also collect information about your family or personal history, where this is relevant to our assessment.

4. Pensions, Savings and Investments

When you purchase an investment product

If you request information for or take out a pensions, savings and investment product with us, we will collect information about your age, retirement age, lifestyle, current state of health, any existing health conditions, details and the value of your pension, savings and/or investments, your employment history, names of your pension schemes, pension scheme numbers, tax information, PPS number, salary, occupation and information on other savings, attitude to financial risk. We may ask you to authorise a healthcare provider to supply relevant supporting information. We need this information to assess risk associated with the policy. We may also collect information about the family or personal history of the insured, where this is relevant to our risk assessment.

5. Business Insurance Including Motor and Non-Motor Business Insurance

When you purchase a policy

If you request a quote for or take out business insurance with us, we will collect information about the company name, the contact person for your company, number of employees, details of employees and their role in the company, details of the business assets to be insured, age, lifestyle, current state of health and any existing conditions of each person included in the policy or proposal. We may ask you to authorise a healthcare provider to supply relevant supporting information. We need this information to assess risk associated with the policy. We may also collect information about the family or personal history of the individuals insured, where this is relevant to our risk assessment. If you take out a business motor policy with us, we will collect information about the driving licence number for each person included in the policy or proposal. We need this information to confirm the licence status of each driver and associated entitlement, Penalty Points and relevant restriction information, and endorsement and conviction details. We do this by validating details against the [IIDS Hub](#) and the [National Vehicle and Driver File \(NVDF\)](#). We will also add details of the policy to the [Motor Third Party Liability Database](#) maintained by the [Motor Insurers Bureau of Ireland \(MIBI\)](#). The MIBI may make this information available to authorised bodies such as the Department of Transport, Tourism and Sport, An Garda Síochána, and The Department of Justice and Equality. We will also provide details of the policy to other authorised bodies, as required by legislation from time to time, such as the Department of Finance.

If you make a claim

If you are making a claim on a business insurance, we will ask you to confirm your identity, provide details of the policyholder and (if different) provide details of the insured, so that we can assess the claim.

- If you are making a claim following a motor accident, we will ask for details of the claim, including for accidents information about those involved and any personal injury you or others may have. We may also validate your claim by checking the licence details of the driver against the [IIDS Hub](#) or the [National Vehicle and Driver File \(NVDF\)](#). We may check your details against the [Insurance Link](#) database maintained by Insurance Ireland.

Credit Checks

For a business policy, we will undertake credit checks on you and/or your business. This will involve disclosing your personal information to credit reference agencies, who carry out searches relating to you.

The Legal Basis for our Use of Information

We will only collect information where we have a lawful basis for doing so. Article 6 of the GDPR defines [six lawful basis](#)' for the collection of data.

The table below sets out the various types of information we collect and process and the legal basis for doing so.

Purpose	Legal Basis
To provide you with a quote for an insurance, Pension or Investment product we sell or service we provide	Processing is necessary for the performance of a contract or in order to take steps at your request prior to entering into a contract
To provide you with insurance cover if you decide to purchase an insurance product with us	Processing is necessary for the performance of a contract or in order to take steps at your request prior to entering into a contract
To provide one of our other financial services to you – e.g. a Pension or Investment	Processing is necessary for the performance of a contract or in order to take steps at your request prior to entering into a contract
To verify your identity	Processing is necessary for the performance of a contract or in order to take steps at your request prior to entering into a contract; To comply with legal obligations (for example money laundering requirements)
To administer your insurance, Pension or Investment contract and make any changes during its term, answer any queries you may have, provide you with updates	Processing is necessary for the performance of a contract
Criminal conviction data is used for the purposes of providing quotes and underwriting, managing reinsurance arrangements, processing any claims you may have, fraud investigation and handling any complaints you may have.	To take steps at your request before we enter into a policy (e.g. providing a quote) and to perform our insurance policy with you and people covered under the policy. We may also need to use your criminal conviction data for the purposes of establishing, exercising or defending legal rights, including in connection with advice, claims, or proceedings, and where authorised by law.
Health data is used for the purposes of providing quotes and underwriting, managing reinsurance arrangements, processing any claims you may have, fraud investigation and handling any complaints you may have.	Irish Data Protection law allows us to use health data in connection with your insurance policy. We may also need to use your health data for the purposes of establishing, exercising or defending legal rights, including in connection with advice, claims, or proceedings, and where authorised by law.
To communicate with you in relation to payments and make and receive any payments in relation to your insurance contract	Irish Data Protection law allows us to use health data in connection with your insurance policy. We may also need to use your health data for the purposes of establishing, exercising or defending legal rights, including in connection with advice, claims, or proceedings, and where authorised by law. Processing is necessary for the performance of a contract
To process a cancellation of your insurance, Pension or Investment contract	Processing is necessary for the performance of a contract
To validate, investigate and/or process any claims you or another person makes in relation to your insurance or Pension contract	Processing is necessary for the performance of a contract

Purpose	Legal Basis
To detect and prevent fraud	Processing is necessary for our legitimate interests
To comply with laws and regulations such as money laundering checks	Processing is necessary to comply with legal obligations
To obtain reinsurance for the business we underwrite	Processing is necessary for our legitimate interests
Personal data	Processing is necessary for the performance of a contract or in order to take steps at your request prior to entering into a contract; Processing is necessary for our legitimate interests
For marketing purposes, including profiling	For our legitimate interests in managing our business.
For management information purposes including portfolio assessment, risk assessment, performance reporting and management reporting.	For our legitimate interests in managing our business.
Market research Data analytics including profiling Staff training Providing online services	For our legitimate interests in managing our business.
in exceptional circumstances where we may use and/or disclose information to protect you, for example, Ward of Court applications or equivalent processes.	To protect your vital interests
Compliance by us with all relevant legal and regulatory obligations to include those (e.g. annual benefit statements, annual reports) if we act as Registered Administrator of a Pension Plan	Processing is necessary to comply with legal obligations

Your Rights

You have legal rights under data protection laws in relation to your personal information.

We may ask you for proof of identity when making a request to exercise any of these rights. We do this to ensure we only disclose information or change account details where we know we are dealing with the right individual.

We will not ask for a fee, unless we think your request is unfounded, repetitive or excessive. Where a fee is necessary, we will inform you before proceeding with your request.

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

We may not always be able to fully address your request, for example if it would impact the duty of confidentiality we owe to others, or if we are otherwise legally entitled to deal with the request in a different way.

1. To access personal information

You can ask us to confirm whether or not we have and are using your personal information.

You can ask to get a copy of your personal information.

2. To correct / erase personal information

You can ask that we rectify any information about you which is incorrect. We will be happy to rectify such information but would need to verify the accuracy of the information first.

You can ask that we erase your personal information if you think we no longer need to use it for the purpose we collected it from you.

You can also ask that we erase your personal information if you have either withdrawn your consent to us using your information (if we originally asked for your consent to use your information), or exercised your right to object to further legitimate use of your information, or where we have used it unlawfully or where we are subject to a legal obligation to erase your personal information.

We may not always be able to comply with your request, for example where we need to keep using your personal information in order to comply with our legal obligation or where we need to use your personal information to establish, exercise or defend legal claims.

3. To restrict our use of personal information

You can ask that we restrict our use of your personal information in certain circumstances, for example

- where you think the information is inaccurate and we need to verify it;
- where our use of your personal information is not lawful but you do not want us to erase it;
- where the information is no longer required for the purposes for which it was collected but we need it to establish, exercise or defend legal claims; or
- where you have objected to our use of your personal information but we still need to verify if we have overriding grounds to use it.

We can continue to use your personal information following a request for restriction where we have your consent to use it; or we need to use it to establish, exercise or defend legal claims, or we need to use it to protect the rights of another individual or a company.

4. To object to how we use personal information

You can object to any use of your personal information which we have justified on the basis of our [legitimate interest](#), if you believe your fundamental rights and freedoms to data protection outweigh our [legitimate interest](#) in using the information. If you raise an objection, we may continue to use the personal information if we can demonstrate that we have compelling [legitimate interests](#) to use the information.

5. To ask us to transfer personal data to another organisation

You can ask us to provide your personal information to you in a structured, commonly used, machine-readable format, or you can ask to have it transferred directly to another [data controller](#) (e.g. another company).

You may only exercise this right where we use your personal information in order to perform a contract with you, or where we asked for your consent to use your personal information. This right does not apply to any personal information which we hold or process outside [automated means](#).

6. To contest decisions based on automated decision making

If we made a decision about you based solely by [automated means](#) (i.e. with no human intervention), and the decision made by us produces a legal effect concerning you (such as the rejection of your claim), or significantly affects you, you may have the right to contest that decision, express your point of view and ask for a human review. These rights do not apply where we are authorised by law to make such decisions and have adopted suitable safeguards in our decision making processes to protect your rights and freedoms.

7. To obtain a copy of our safety measures

You can ask for a copy of, or reference to, the safeguards we have put in place when your personal information is transferred outside of the European Economic Area. We are not required to share details of these safeguards where sharing such details would affect our commercial position, or create a security risk.

8. To withdraw consent

Where we rely on your consent as our legal basis for use of your personal data you have a right to withdraw your consent to such use.

Contact Us

Please contact us

The primary point of contact for all issues arising from this privacy policy, including requests to exercise data subject rights, is our Data Protection Officer, Brian O'Connor. The Data Protection Officer can be contacted in the following ways:

email address - brian.oconnor@aviva.com

postal address - Aviva Insurance Group, One Park Place, Hatch St, Dublin 2, Ireland.

Our supervisory authority

If you are not happy with the way we are handling your information, you have a right to lodge a complaint with your local data protection supervisory authority at any time. In Ireland this is the Office of the Data Protection Commission,

Email address – info@dataprotection.ie

Postal address - Canal House, Station Rd, Portarlinton, Co Laois.

We ask that you please attempt to resolve any issues with us before contacting the office of the Data Protection Commissioner.

List of Aviva Group Companies

This Policy applies to the following Aviva companies operating in the Republic of Ireland.

Aviva Life & Pensions Ireland DAC a company incorporated in Ireland with company number 165970;

Aviva Life Services Ireland Ltd a company incorporated in the Republic of Ireland with company number 406616;

Aviva Direct Ireland Ltd a company incorporated in the Republic of Ireland with company number 374895;

Aviva Driving School Ireland Ltd a company incorporated in the Republic of Ireland with company number 429195;

Aviva Trustee Company Ireland Ltd a company incorporated in the Republic of Ireland with company number 23751;

Aviva Group Services Ireland Ltd a company incorporated in the Republic of Ireland with company number 322579;

Aviva Insurance Ireland DAC a company incorporated in the Republic of Ireland with company number 605769.

Details about the Aviva Group of companies outside the Republic of Ireland can be found on www.aviva.com.

Definitions

Automated Means: a decision made without any human involvement

Consumer Protection Code: a set of rules and principles that all regulated financial services firms must follow when providing financial products and services to consumers.

Data Controller: the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.

Direct Marketing: a form of advertising where organisations communicate directly to customers through a variety of media.

European Economic Area (EEA): The European Economic Area (EEA) unites the EU Member States and the three EEA EFTA States (Iceland, Liechtenstein, and Norway) into an Internal Market governed by the same basic rules. These rules aim to enable goods, services, capital, and persons to move freely about the EEA in an open and competitive environment, a concept referred to as the four freedoms.

Financial Crime: this includes bribery and corruption, fraud, facilitation of tax evasion, market abuse, money laundering and terrorist financing, sanctions violations

GDPR: General Data Protection Regulations

IIDS Hub: Integrated Information Data Service. Shared members' database allowing users to confirm the accuracy of penalty point and no-claims discount information provided by customer when they are seeking motor policies.

Insurance Link: this is a database that was created to assist members in the detection and defence of exaggerated claims which may result in prosecutions for fraud. This website can be found by clicking on the following link: <https://www.inslink.ie/>

Lawful basis for processing: GDPR defines 6 lawful basis for processing:

Consent - the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

Performance of a contract - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

Legal obligation - processing is necessary for compliance with a legal obligation to which the controller is subject;

Vital interests - processing is necessary in order to protect the vital interests of the data subject or of another natural person;

Public interest - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

Legitimate interest - processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental

rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Motor Insurers Bureau of Ireland (MIBI): a non-profit making organisation who compensate victims of road traffic accidents caused by uninsured and unidentified vehicles.

Motor Third Party Liability Database: a database that tracks annual claims and analyses a trend in motor insurance claims.

National Vehicle and Driver File (NVDF): a database containing details of all registered vehicles and their owners as well as the licensed drivers in the country.

Past or Pending Offences: a breach of law, either past or present

Payment details: bank account details which include account name, IBAN and BIC number.

Prevent fraud: prevent the wrongful or criminal deception intended to result in financial or personal gain.

Processes: any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Spent convictions – Criminal convictions that do not need to be declared under the terms of the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016.

Telematics Data: the field of science that deals with long-distance transmission of computer-based information using GPS satellites and receivers.

Vital Interests: life or death scenarios.

