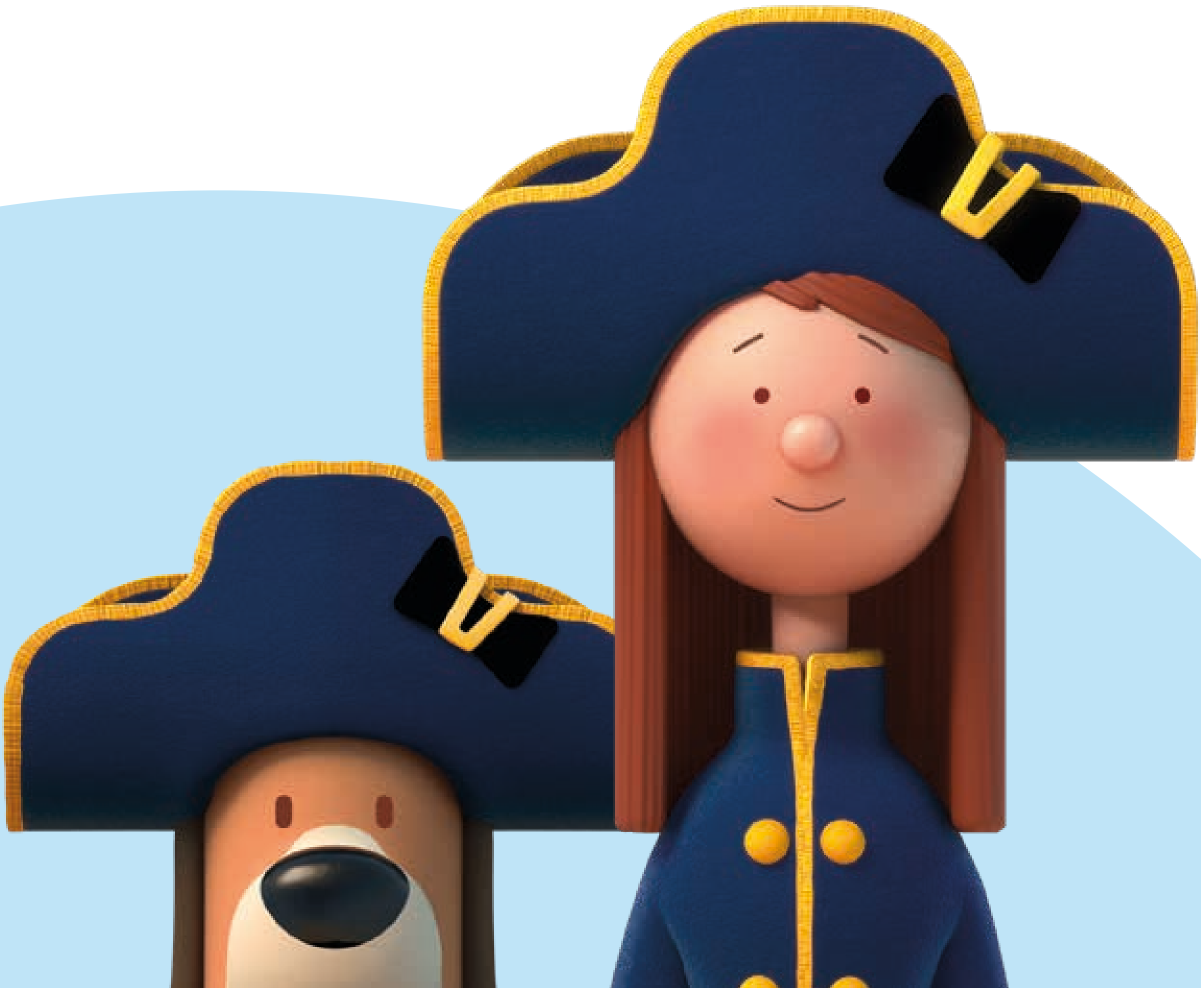
Our privacy policy

Committed to protecting your personal data

Last updated 8th June 2026



Contents

We know your privacy is important - really important. That's why we always treat your personal data with the respect it deserves and share with you how we do that.

Let's talk privacy

Our privacy policy is here to help you understand how we collect, use and protect your data.

It applies when:

- you buy a policy or product from us
- you get a quote for a policy or product
- another organisation gives us your personal data
- you contact us to deal with a policy or product (for example, to make a change to your policy)

Every now and then, we introduce new services or products. They'll also be covered by our privacy policy, unless we say otherwise when we launch them.

Just a heads up…

If you're looking for your policy information, or anything specific about our different products, you're in the wrong place - sorry! Log in to your online account or check out our policy documents page for more information.

Need help quick?

You'll find all the information about how we use your personal data in this privacy policy. But here's a quick overview of some key information you might be looking for:

Make a Subject Access Request (SAR): To get access to your personal data, contact the Information Rights Team.

Marketing preferences: You can opt out of marketing when you get a quote or buy from us. Or you can opt out anytime by emailing us or clicking 'unsubscribe' in any marketing emails.

Contact our Data Protection Officer (DPO): If you have any questions, concerns or feedback about this policy or how we handle personal data, email us.

If you need this policy in any other format or have any accessibility needs, check out our help and support hub.

Changes to this policy

We might make changes to the policy. When we do, we'll always make sure to tell you about any important changes.

For example, we might show a notice in your Admiral account, send you an email, or send a notification on your device.

Ready to dive in? Carry on reading to find out more about how we look after your data.

What is the Admiral Group, and what do we do?

Our brands and companies

While you probably know us as a car insurer, we do a whole lot more than that! In fact, the Admiral Group is made up of all sorts of different brands and companies, including:

EUI Limited (Registered Number 02686904) which includes the trading names Admiral, Diamond, Bell, MoreThan, Elephant and Gladiator.

Able Insurance Services Limited (Registered Number 02890075) which includes the trading names Veygo, Pioneer, Admiral Business

Admiral Law Limited (Registered 08023665) which includes the trading names Admiral Law, EUI Law, Diamond Law, Elephant Law and BDE Law

Admiral Financial Services Limited (Registered 10255225) which includes the trading names Admiral Money, Admiral Mortgages, Admiral Loans, Admiral Car Finance, Admiral One, Finble.

Our privacy policy applies to any of our UK companies that you get a quote, or buy a policy or product from. That company is known as the 'data controller', and they're dedicated to handling your personal data according to everything in this privacy policy.

Find out more about how we share your personal data within the Admiral Group.

A quick bit of housekeeping

When we refer to 'Admiral', 'us', 'we' or 'our' in this privacy policy, we're talking about the relevant data controller within the Admiral Group.

If you're not sure who's the relevant data controller of your personal data, let us know at DPOoffice@admiralgroup.co.uk and we'll be happy to point you in the right direction.

Other data controllers

While we're here, there's a few more data controllers who might be involved in processing your personal data.

That's because they're companies we work with closely, or who are involved with some of the products and services we offer.

They include:

- **Telematics (Dependent on product):** Octo Telematics S.p.A, Drive Factor Inc., Vodafone Automotive UK Limited (3751493), Redtail Telematics Ltd (Registered Number 07407204).
- **Pet Insurance:** Ultimate Insurance Solutions Limited (Registered Number 03299891).
- **Motor Insurance:** Great Lakes Insurance SE (Registered Number HRB 230378), Admiral Insurance (Gibraltar) Limited/ Admiral Insurance Company Limited.
- **Ford Insure:** FCE Bank plc (Registered number 772784).
- **GAP Insurance:** Car Care Plan Ltd (Registered Number 850195)

Wondering which other companies might get your personal data? Head over to our page on sharing your personal data.

Your personal data rights

The UK has some strong privacy laws that give you control over how your personal data is collected, used and shared. And we think it's important that you know exactly what they are, and how they apply to you.

These laws include (but aren't limited to):

- The UK General Data Protection Regulation (you'll probably know this as the GDPR!)
- The Data Protection Act 2018
- The Data (Use and Access) Act 2025

Here's a breakdown of:

- your rights
- when they apply
- and how you can exercise them

You have a right to:		**How?**
Be informed	Know what personal data we process about you and how we process it.	We keep you informed: • through this privacy policy • through the information we give you when you buy a policy or product with us • by answering your questions and requests when you get in touch
Make a Subject Access Request ("SAR")	Ask for access to the personal data we process about you, as well as certain other information about how we process it	To ask for access to your personal data, you can email us at InformationRightsTeam@admiralgroup.co.uk or give us a call.
Rectification	Ask that we change or update your personal data if it's inaccurate or incomplete.	You can update your details at any time by getting in touch with us or in your online account.

You have a right to:		How?
Erasure	• Ask us to delete your personal data in some situations. • For example, you can ask us to delete personal data: • we no longer need for the reason we collected it • we process based on the legal basis of consent, and you withdraw your consent • when you object (check out our section on objecting below) and • if we have processed it unlawfully • there are no overriding legitimate grounds for us to keep your personal data • or you object to how we've processed your personal data for direct marketing purposes Just a heads up, there are some situations where we won't be able to delete your data. For example: • when it's still necessary for us to process your personal data for the reason we collected it (for instance, so we can give you a service) • when we have legitimate grounds to use your personal data which override your interest to delete it (for example, where we need the data to protect ourselves from fraud) • when we have a legal obligation to keep the data (for example, to help prevent money laundering) • when we need the data to support or defend legal claims (for example, if there's an issue with your account and we haven't been able to resolve yet)	You can ask us to delete your personal data by emailing us at InformationRightsTeam@admiralgroup.co.uk

<table>
<tr><th colspan="2">You have a right to:</th><th>How?</th></tr>
<tr><td>Restriction</td><td>Ask us to restrict our processing of all, or some, of your personal data.

You can do this if:
• your personal data isn’t accurate
• we processed it unlawfully
• we don’t need your personal data for a specific reason
• you object to how we process it, and we’re assessing your objection request - check out our section on objecting below

You can ask that we restrict processing your data either temporarily or permanently.

Just so you know - unless there is a valid request to restrict your personal data being processed, we might:
• continue to store your personal data
• process it with your consent
• use it to support or defend a legal claim (for example, if there’s an issue with your account and we haven’t been able to resolve yet)</td><td>You can make an objection request by contacting us at InformationRightsTeam@admiralgroup.co.uk

You can unsubscribe from direct marketing at any time by:
• clicking ‘unsubscribe’ on any direct marketing email from us
• emailing marketingpreferences@admiralgroup.co.uk
• writing to Head of Customer Assurance, Ty Admiral, David Street, Cardiff, CF10 2AA</td></tr>
<tr><td>Data portability</td><td>Ask us to transmit your personal data to a third party.

You have the right to get your personal data in an electronic format, and the right to transmit your data to a third party for use in that third party’s service.

Just so you know - if you’d like, we’ll give you an electronic copy of your data to pass onto third parties.
But right now, we can’t send your information directly on to a third party.</td><td>For more information see our section on access above.</td></tr>
</table>

You have a right to:		How?
Not be subject to automated decision making	Have a human involved when a decision is going to be made that would have a legal or significant effect on you. This right doesn't apply if: • the decision is needed to enter into, or perform, a contract between you and us • it's authorised by law • we have your explicit consent. In those cases, you do still have a right to request human intervention. So don't hesitate to let us know your views and challenge the decision!	You can ask for more information about how we make decisions about you by getting in touch. Find out more about automated decision making.
To make a complaint	You have the right to make a complaint about any concerns you have on how we process your personal data. You can raise your complaint with the Information Commissioner's Office	Find out how to raise a complaint with the DPO and find the ICO details here.

Got more questions?

Do I have to pay to make a information rights request?

In most cases, you don't have to pay to exercise your rights.

How long does it take once I've made a privacy request?

Once you've made a request to us about your data, we have one month to respond.

In some situations, we can extend it by another two months.

What personal data we collect about you

We have to collect some data about you to be able to look after you properly.

For example, we can't set you up with an insurance policy if we don't know your name, or an email address to send your documents.

Here's a breakdown of the different categories of data we collect.

What data we collect when you get a quote, or buy a policy or product

The data we need to set up your account or get you a quote

Personal data that we need to set you up with a policy or product. This includes:

- Contact details, including your name, email address, address and phone number
- Date of birth
- Gender
- Marital status
- Employment status
- Special category data, including medical information and criminal convictions (for example, if you need us to make any reasonable adjustments to support you based on your needs)
- Machine identifiers, including your IP address
- Telematics information, including your location, car information and driving details (see our section on telematics)
- App information, including event data and the time and date you got a quote
- Information about your income
- Proof of residency
- Financial information, like your bank details, credit card details, and information we've got from any credit checks, bankruptcies and other financial information, like county court judgements
- Transactional data (for example, insurance claims or details about payments to and from your accounts)
- Information we've got through our use of cookies and other tracking technologies - you can find out more about this in our cookie policy
- Details of any vulnerabilities you might have, and the support we can offer
- ID documents, including photographs and videos, which may include biometric data

Details about you as a driver

- Details of any named drivers on the policy, and their relationship to you as the policyholder
- Driving license
- No claims bonus
- Claims history
- Related third party details if you're involved in a claim

Property information

- Registration plate (also known as a number plate)
- Car details
- Property information, like the type of building, any features, etc

Details about anyone else involved

- Contact details of third parties associated with your policy or product (for example, a named driver)
- Driving history of third parties
- Any nominated representatives or authorised callers
- If you give us personal data about someone else, you're acknowledging:
- that you have their permission to do so
- that they understand how we'll process their data
- We'd strongly encourage anyone whose personal data you give us to read this privacy notice, so they understand everything fully.

Marketing information

- Data collected through our use of cookies and other tracking technologies on our websites and apps (for example, IP address, cookie ID and device information)
- Your marketing preferences
- Advertising profile, including the products you're most likely to be interested in based on your product information

What data we collect when you contact us or make a claim

Customer service data

- Voice recordings of calls made to our call centres
- Webchat and transcripts when you contact our customer care team
- Emails to our customer care team

Just a heads up - we might record conversations for training and quality purposes.

Claims data

- About where the incident happened
- Claim evidence (for example, photos of claim details, dashcam footage, CCTV or automatic number plate recognition)
- Information from your car's on-board diagnostics device or telematics app (for example, the location, speed, distance driven, mileage reading, and cornering and braking if you're a telematics customer)
- Details of any injuries
- Some of these details might include other people who were involved, like partners or children

What data we collect if you have a telematics policy

Using our telematics product

If you use our telematics product we'll collect vehicle and driving related data from your vehicle.

That includes:

1. Date and time
2. Location (latitude and longitude)
3. Speed, distance, and duration
4. Acceleration, braking, and cornering
5. Other vehicle-related information

We usually record data while you're using your vehicle. It's sent to us after a short delay by our trusted partners who provide and deal with telematics products.

Third party sources that we get your data from

Open internet and device information

We collect some information from internet sources like:

- The Open Government Licence
- Internet searches
- Marketing companies who give us policy renewal information
- News articles
- Online marketplaces
- Social media platforms
- Details from the devices and networks you use to interact with our apps or websites
- Telematics data from the use of cookies and app information (check out our cookie policy for more info)

This information helps manage our fraud and pricing processes that we talk about in our section on the data we collect about you.

What type of data we get from them

- Road tax status
- Geological or flood data for your area
- How much your home is worth
- Social media information
- Mobile information such as device type, IP address and operating system

Motor Insurance Bureau

We work with the Motor Insurers' Bureau (MIB) - and some associated, not-for-profit companies - who do lots of services for the insurance industry.

At every stage of your insurance journey, the MIB will be processing your personal information. To find out more, head to the MIB website.

Here's a quick overview of the type of activity the MIB does:

- Checking your driving licence number against the DVLA driver database to get driving licence data (including any driving conviction data) to help calculate your quote and tackle fraud
- Checking your no claims bonus and claims history
- Preventing, detecting and investigating fraud and other crime by carrying out fraud checks
- Maintaining databases of:
  - Insured vehicles (Motor Insurance & Policy Data, or Motor Insurance Database)
  - Vehicles that are stolen or not legally allowed on the road (Vehicle Salvage & Theft Data, or MIAFTR)
  - Motor, personal injury and home claims (CUE)
  - Employers' Liability Insurance Policies (Employers' Liability Database)
- Managing insurance claims that relate to untraced and uninsured drivers in the UK and abroad
- Working with law enforcement to stop uninsured vehicles being used on the roads
- Supporting insurance claims processes
- What type of data we get from them
- No claims bonus
- Driver details

What type of data we get from them

- No claims bonus
- Driver details

DVLA

We might collect your driving licence number (DLN or 'MyLicence') when you apply for motor insurance or when you make a claim. In some cases, we might not be able to insure you without that information.

We use your driving license number to do an automatic check with the Driver and Vehicle Licensing Agency (DVLA) driver database.

We might use the DVLA's data, and any other information you've given us, to:

- calculate a motor insurance quote for you
- take care of your policy
- help prevent fraud

We won't use the data for any other reason or share it with anyone else. Only the motor insurance industry can use this information.

If you apply for a quote and then decide not to take out insurance with us, the data we get from the DVLA database will be made anonymous or deleted no later than 30 days after we get it.

We might carry out searches before your insurance policy starts and at any point throughout your policy, as well as when you renew.

For details about the information the DVLA holds about you, head to www.dvla.gov.uk and www.mylicence.org.uk.

To see your driving licence, visit www.gov.uk/view-driving-licence.

What type of data we get from them

- What type of licence you have
- How long you've held your license for
- Entitlements to drive
- Penalty points
- Convictions
- Conviction dates
- Disqualifications

Credit Reference Agencies

TransUnion: Consumer Services Team, PO Box 647, Unit 4, Hull, HU9 9QZ or call **0330 024 7574** or email UKConsumer@transunion.com.

Equifax: Credit File Advice Centre, PO Box 1140, Bradford, BD1 5US or call **0844 355 0550** or log on to www.equifax.co.uk.

Experian: Consumer Help Service, PO Box 8000, Nottingham, NG80 7WF or call **0844 481 8000** or log on to www.experian.co.uk.

We do some checks when you:

- open an account
- renew your policy
- ask for a change to your insurance agreement

We do this to assess your application for credit and to check your identity. This helps us to spot and prevent crime, including money laundering.

We might also check the details you give us when you buy your policy, renew it, or apply for a financial agreement. This is to work out any misrepresentation and to prevent insurance fraud if you make a claim.

To get this information, we'll check some records about you, anyone else who might be insured with us, or a joint party whose personal details you've given us as part of your application.

Those records include:

- Our own records
- Credit Reference Agency (CRA) records. When CRAs get a search from us, they'll put a 'search footprint' on your credit file that other lenders might see. CRAs give us both public (including the electoral register) and shared credit and fraud prevention information.
- Fraud Prevention Agency (FPA) records
- We make searches about you at credit reference agencies, who give us information including the Electoral Register and credit information. The agencies will record details of the search whether or not your application goes ahead.

The searches won't be seen or used by lenders to assess if you can get credit from them.

We might use scoring methods to check your application and verify your identity.

When you or someone in your household applies for things like insurance or loans, we and other companies might use credit checks and other information we've been given about you or anyone you're financially linked to.

We might also use this information to:

- trace debt
- prevent money laundering
- manage your account

We could also ask you to give us a physical form of identification.

If you're making a joint application, or you want to tell us that you have a spouse or financial associate, we'll link your records together. That's why it's important to make sure they agree you can share their information with us!

CRAs will also link your records together. These links will stay on both your files until either of you successfully file for a 'disassociation'. That means the link would be removed from your files.

We might also make regular searches at CRAs and FPAs to manage your account and offers with us.

Information on applications will be sent to and recorded by CRAs. When you borrow from us, we'll give details of your account(s) and how you manage them to CRAs. If you borrow from us and don't repay the money in full and on time, CRAs will record the outstanding debt.

CRAs and FPAs might then give that information to other organisations to do similar checks, trace where you are, and recover any debts that you owe. These records stay on file for six years after they're closed, whether you settle them or are defaulted (that's when you don't pay them at all).

If you give us false or inaccurate information and we suspect or identify fraud, we'll record it. We might also pass this information to FPAs and other organisations that are involved in preventing crime and fraud.

If you borrow from us and don't make payments that you owe us, we'll trace where you are and recover your debts.

If we or a fraud prevention agency decide you pose a fraud or money laundering risk, we might:

- refuse to offer the services and financing you've requested
- refuse to employ you
- stop providing existing services to you

Fraud prevention agencies will keep a record of if you're a fraud or money laundering risk. It could mean others refuse to offer you services, financing or employment. If you have any questions about this, get in touch using the details below.

Your data might also be used for other purposes that you give your specific permission for, when we have legitimate business interest, or when it's required by law or under the terms of the GDPR.

Still got questions? Get in touch

This is a short guide to how we use your personal information when it comes to credit referencing. If you'd like to read the full details of how your data might be used, you can:

- give us a call on **0333 220 2062**
- write to us at Pricing Department, Ty Admiral, David Street, Cardiff, CF10 2EH

You can also get in touch with the CRAs that are currently working in the UK. They might not all have the same information, so you might need to contact them all. They'll charge you a small fee.

What type of data we get from them

- Electoral Register Information
- Credit information

Open banking

Admiral Money: Moneyhub Financial Technology Limited, Roxburgh Milkins Limited Merchants House North, Wapping Road, Bristol, United Kingdom, BS1 4RW. Check out Moneyhub's privacy policy.

Admiral Pioneer: Trustly Group AB, Rådmansgatan 40, floor 5, 113 57 Stockholm, Sweden. Check out Trustly's privacy policy.

We might ask you to share access to your bank or building society account data through Open Banking:

- when you apply for something with us (for example, a loan or other financial product)
- during your agreement with us
- sorting out settlement payments for you
- helping us check the product we offer is right for you, or still meets your needs if your circumstances change

Open Banking lets you share your bank or building society account data securely. That's because it's through an FCA-regulated Account Information Service Provider (AISP).

We'll put you safely in touch with an AISP, who work with UK banks and building societies to give secure access to your information.

Before you give your permission, you'll be told who the AISP are and get a link to their privacy policy.

Once you've given your permission, they'll collect information from your bank or building society account(s), which we can then access and use securely.

If you're applying for a loan or other product, we'll get two years of information from your main bank account and any other accounts you've chosen. This will be two years from the date you agreed to give us access.

Once you've given us access, we can review the information we have within the next 90 days. For example, when you've agreed an arrangement with us, we'll be able to review it to see if it's still right for you.

After this 90-day period, we'll ask for your permission if we need to access your information again.

You can remove our access to your bank or building society accounts at any time by getting in touch with us.

When you share this data with us, we might use the information to:

- consider whether you can afford the loan or other financial product you're interested in
- check if any other information you've given us is accurate
- manage your relationship with us
- help us understand how your circumstances might have changed
- help us prevent criminal activity and financial crime, including fraud and money laundering
- process payments for you after a claim settlement or another similar payment process

We might also use your personal information to:

- create and improve the products and services we offer
- develop and improve our processes, credit risk system and policies

This is so we can meet the needs of our customers better.

We might also use this data, alongside information we've got from credit reference agencies and other organisations, to do some 'analytical modelling'. This means we look at your characteristics, interactions and behaviours to profile your information.

It helps us work out what the appetite for risk is when it comes to lending to you or making another arrangement with you. If your information shows you might not be likely to pay us back in full, it might be a higher risk for us to lend to you.

We'll continue to do this whether either of us chooses to go ahead with your application, arrangement, or if you continue to be one of our customers.

Some other things to know about Open Banking:

If you give us access to a joint bank account, we and AISPs that we work with might also have access to data about your spouse, partner or other financial associate. Open Banking says that any of the holders of a joint bank or building society account can grant access to this.

When we're lending or offering other financial services, it's our responsibility to make sure the products we give you are affordable and meet your needs.

To do this, we securely share your payment information with credit reference agencies to make sure we have enough data to make well-informed decisions about offering credit.

It also helps the rest of the financial sector get a better understanding of your credit history and accounts. This means they can also make sure you're only offered financial services you can afford.

As well as managing access to your bank and building society account(s), AISPs might use the information they get for their own reasons.

What type of data we get from them

- Name, number and sort-code
- Balances, and any incoming or outgoing transactions
- Fees, charges, interest, benefits or rewards
- Regular payments, like standing orders and direct debits

Price comparison websites & other third parties

We might share your personal data with some other organisations who help us handle your insurance or other financial products, including:

- price comparison websites (PCWs) - we might match your PCW quote to your customer profile, so we can tailor offers to you
- other insurers
- re-insurers
- brokers
- some other third parties

What type of data we get from them

- Name
- Account Details
- Policy details

Price comparison websites & other third parties

We might share your personal data with some other organisations who help us handle your insurance or other financial products, including:

- price comparison websites (PCWs) - we might match your PCW quote to your customer profile, so we can tailor offers to you
- other insurers
- re-insurers
- brokers
- some other third parties

What type of data we get from them

- Name
- Account Details
- Policy details

Why do we use your personal data?

Our legal reasons for collecting your data

We don't just want you to know what personal data we collect - we think it's important that you understand why we collect it too.

Below, we explain:

- why we use your personal data (the purpose)
- our legal justifications (each called a 'lawful basis') for collecting your data under data protection law, depending on why we've collected it
- what each category means for why we collect your personal data - find out more about the personal data we collect about you

Here's a quick explanation of each 'lawful basis' to help you understand a little easier:

Performance of a contract

This is when we (or a company we're working with) need to use your personal information to meet the terms of a contract with you, or to do things you've asked for before we make a contract.

This includes us using your personal information to give you the service agreed in your policy or product terms and conditions, or to check details before starting a new one with you.

Legitimate Interest

This is when we, or another company working with us, has a legitimate reason (for example, a commercial interest) to use your personal information.

It only applies when the reason isn't overridden by your interests, rights or freedoms. For example, we might use your policy information to better calculate the cost of your insurance.

Get in touch if you want to understand anything in more detail.

Consent

This is when you actively agree to us using your personal data for a certain purpose. You can withdraw your consent whenever you want.

Compliance with legal obligations

This is when we have to process your personal data to comply with a law.

Why we collect your data – the 'purpose' for processing your data	The 'legal basis' that lets us to collect data for that purpose	The categories of personal data used for the purpose
Processing your policy quotes or finance application	Performance of contract	• Account and quote data • Customer service data • Related third-party details • Driver details • Property Information
Looking after your policy or finance agreement, resolving complaints, handling claims, and giving you ancillary products, like breakdown cover	Performance of contract	• Account and quote data • Claims data • Customer service data • Related third party details
Call recording and monitoring	**Legitimate interests** - We monitor or record calls, emails, SMS messages and other communications for business purposes, like quality control and training **Compliance with legal obligations** - e.g. Anti Money Laundering **Protecting your vital interests** - e.g. recording and passing on your details in a medical emergency	• Account and quote data • Customer service data • Related third-party details • Driver details • Property information • Voice data • Health information • Political or religious beliefs • Sensitive data

Why we collect your data – the 'purpose' for processing your data	The 'legal basis' that lets us to collect data for that purpose	The categories of personal data used for the purpose
Detecting and preventing fraud across the Admiral Group	**Legitimate interests** - it's important for us to check the information we get is true and stop fraudulent claims. **Compliance with legal obligations** - e.g. Anti Money Laundering.	• Account and quote data • Customer service data • Related third-party details • Driver details • Property information • Claims data • ID documents
Credit scoring	**Legitimate interests** - it's important for us to check the risk level of selling a certain product to someone. For example, if someone has a very low credit score and a history of not paying back loans, it might be too much of a risk to lend to them or give them insurance.	• Account and quote data
Debt recovery or other legal claims	**Legitimate interests** - it's reasonable for us to get back any money we're owed, as well as bringing or defending any legal claims.	• Account and quote data
Checking your identity when we need to	**Compliance with legal obligations** - e.g. Anti Money Laundering	• Account and quote data
Doing market research, product development and statistical analysis	**Legitimate interests** - we have a legitimate interest in analysing and growing our business, and developing our products and services.	• Account and quote data
Processing the auto-renewal of your policy	Performance of a contract	• Account and quote data • Customer service data • Related third-party details • Driver details • Property information • Claims data

Why we collect your data – the ‘purpose’ for processing your data	The ‘legal basis’ that lets us to collect data for that purpose	The categories of personal data used for the purpose
For assessment and analysis to let us review, develop and improve the services we offer	**Legitimate interests** - we have a legitimate interest in analysing and growing our business, and developing our products and services.	• Account and quote data • Customer service data • Related third-party details • Driver details • Property information • Claims data
Telematics	**Performance of contract** - we and our trusted partners use telematics data for: 1. Insurance calculations - deciding how much your insurance costs based on how you use your vehicle, and creating driving scores 2. Providing you with services related to the policy 3. Device support - installation, activation, servicing, updates, and testing 4. Contacting you about your policy or telematics device via post, email, phone, or SMS **Legitimate interests** - 1. managing claims 2. preventing and detecting fraud 3. research & analysis to improve our services **Protecting your vital interests** - If the device detects a serious crash, we’ll try to contact the policyholder and named drivers. If we can’t reach anyone, we’ll share details with emergency services, including the vehicle’s last known location and names on the policy.	• Date and time • Location (latitude and longitude) • Speed, distance, and duration • Acceleration, braking, and cornering • Other vehicle-related information

Why we collect your data – the ‘purpose’ for processing your data	The ‘legal basis’ that lets us to collect data for that purpose	The categories of personal data used for the purpose
Refining our pricing models using data we’ve collected, quote data and data from external sources including credit reference agencies	We use it to: • refine our pricing and risk assessment models across all our products - this just means how we work out the cost of your product, and check if we can offer it to you • improve how accurate the cost of our insurance is • improve the quality of our services The ‘legal basis’ that lets us collect data for that purpose **Legitimate interests** - we have a legitimate interest in analysing and growing our business, and developing our products and services.	• Account and quote data • Customer service data • Related third-party details • Driver details • Property information • Claims data
Internally auditing our processes to maintain our high standards	The ‘legal basis’ that lets us collect data for that purpose **Legitimate interests** - we have a legitimate interest in analysing and growing our business, and developing our products and services.	• Account and quote data • Customer service data • Related third-party details • Driver details • Property information • Claims data

Why we collect your data – the 'purpose' for processing your data	The 'legal basis' that lets us to collect data for that purpose	The categories of personal data used for the purpose
Surveys	The 'legal basis' that lets us collect data for that purpose Consent - We might sometimes get in touch to ask you to take party in a survey. These are designed to help us review, develop and improve our services. We usually use a third-party supplier to host our surveys, which means they're processing some data for us. Any third-party survey tools we use will have their own privacy policies. We recommend reading these before filling out a survey on those platforms. You can withdraw your consent whenever you want, by contacting marketingpreferences@admiralgroup.co.uk	• Account and quote data
Direct marketing - contacting you directly about offers through email or online targeted advertisements	Consent	• Account and quote data • Marketing information
To create profiles to consider what products and services you might be interested in	**Legitimate interests** - we have a legitimate interest in growing our business by marketing our range of products and services to existing customers.	• Account and quote data • Marketing information
To screen individuals against marketing lists for certain products (for example, loans) and to advertise products to eligible customers	**Legitimate interests** - we have a legitimate interest in growing our business by marketing our range of products and services to existing customers.	• Account and quote data

Sharing your personal data

Who we share your data with

Sometimes we need to share your personal data with other companies. But we want you to understand what we share and why we share it.

Some of these companies might be the 'data controllers' we mentioned earlier. They'll decide for themselves how and why they process your data. Others are our data processers, meaning they're under strict instructions to do things our way!

In both situations, we make sure that any data we share is passed along securely with plenty of safeguards in place. And, more importantly, that it's never shared for a reason you haven't been told about.

Companies within the Admiral Group

Check out our full list of companies in the Admiral Group.

What type of data we share with them

- Account and quote data
- Customer service data
- Related third-party details
- Driver details
- Property information
- Claims data
- Marketing information

Why we share your data

To help find and stop fraud, we might share information about you with other companies in the Admiral Group.

We might also do this so we can automatically fill your details in when you use another Admiral product, saving you the hassle of having to type them in again.

That includes Admiral Law - head over to the Admiral Law website for more details.

Motor Insurance Bureau

You can check that the MIB has your correct registration number details by:

- visiting www.askmid.com
- writing to: Motor Insurers' Bureau, Linford Wood House, 6-12 Capital Drive, Milton Keynes, MK14 6XT

What type of data we share with them

Account and quote data

Why we share your data

We pass information to:

- the Claims and Underwriting Exchange Register
- the Motor Insurance Anti-Fraud and Theft Register

These are both managed by the Motor Insurance Bureau (MIB).

This helps insurers check information and stop fraudulent claims.

We might search these registers when you apply for insurance.

You need to tell us about any incident, like an accident or theft, that might turn into a claim. When you tell us about an incident or accident, we'll pass this information to the Registers.

We'll add information about your motor insurance policy to the Motor Insurance Database (MID), which is managed by the Motor Insurers' Bureau (MIB).

MID, and the data stored on it, might be used by some statutory and/or authorised bodies including:

- the police
- the Driver and Vehicle Licensing Agency (DVLA)
- the Driver and Vehicle Agency Northern Ireland (DVANI)
- the Insurance Fraud Bureau

They're legally allowed by law to use it for a few reasons, including:

- electronic licensing
- continuous insurance enforcement
- law enforcement - to find and prosecute offenders
- providing government services and/or other services that are aimed at reducing the level of uninsured driving

If you're involved in a road traffic accident (either in the UK, the EEA or certain other territories), insurers and/or the MIB may search the MID to find some relevant information about you.

If you're involved in a road traffic accident, you (or someone acting on your behalf) might be able to access relevant information held on the MID. That includes citizens of other countries.

It's really important that your correct registration number is listed on the MID.

If it's wrong, the police might think your vehicle isn't insured which could lead to it being seized.

Fraud prevention agencies

These include CIFAS (Fair Processing Notice), Insurance Fraud Bureau, Lexis Nexis.

What type of data we share with them

- Account and quote data
- Customer service data
- Related third-party details
- Driver details
- Property information
- Claims data
- No claims history

Why we share your data

We'll share the personal information we've collected from you with fraud prevention agencies. This is so they can use it to help stop fraud and money laundering, and to confirm your identity.

If you give us false or wrong information and we identify fraud, we'll pass your details to fraud prevention agencies. Law enforcement agencies (like the police) might access and use this information.

We and other organisations might also access and use this information to stop fraud and money laundering. For example, when:

- checking your details when you apply for credit and credit-related services
- managing credit and credit-related accounts
- recovering debt
- checking details on proposals and claims for all types of insurance
- checking the details of people who apply to work with us or our employees

Claims suppliers

What type of data we share with them

- Claims data

Why we share your data

We might share your personal data with claims suppliers and companies that help us when dealing with your claim.

This could include:

- loss adjusters
- claims administrators
- our approved repairers' network
- medical professionals
- any company representing third parties to the claim

These include (but aren't limited to) Auxillis Services Limited and the AA Limited.

Survey providers

What type of data we share with them

- Account and quote data

Why we share your data

When you've agreed to take part in a survey, we might share your data with some carefully chosen third parties to help give you the survey.

These include UserTesting Group and QuestionPro.

LivePerson

What type of data we share with them

- Account and quote data
- Customer service data

Why we share your data

We share your personal data with LivePerson so they can keep our web messaging up and running.

Regulatory bodies (like the Prudential Regulation Authority, Information Commissioner's Office, the Financial Conduct Authority, and the Financial Services Ombudsman)

What type of data we share with them

- Account and quote data
- Customer service data
- Related third-party details
- Driver details
- Property information
- Claims data

Why we share your data

Your personal data might be shared with regulatory bodies if we need to respond to any requests from them

Vehicle manufacturers

What type of data we share with them

- Customer service data

Why we share your data

We might share your data with vehicle manufacturers to organise safety recall alerts.

FCE Bank Plc

What type of data we share with them

- Account and quote data
- Why we share your data

We'll share your personal information with FCE Bank plc for:

- complaints handling
- reporting
- audit reasons

If the provider of Ford Insurer changes, FCE Bank plc will also become a data controller for any personal data given to EUI.

FCE Bank plc will tell your new provider to get in touch with you before your policy renews.

Check out FCE Bank plc's privacy policy, so you can find some more information on how they use your personal data.

Providers of marketing and advertising services

What type of data we share with them

- Email address or contact details (this info will be hashed, which basically means it's encrypted to protect your privacy)
- Information collected through our use of cookies and other tracking technologies on our websites and apps

Why we share your data

We'll share your personal data with marketing and advertising companies. These include social media platforms,media agencies, and advertising technology companies. This is so they can deliver marketing and advertising that's relevant to you.

It's also so we can analyse and measure how successful our marketing campaigns have been (which keeps our Marketing team happy).

Find out more about how we keep your personal data safe.

Other times we share your data

There might also be some more situations where we share your personal data with other companies - but we only ever do this if there's a lawful basis for us to. At every step, we follow strict privacy standards to keep your information safe.

Some examples include:

- Adding information to our data from external databases, so we can give you a quote. For example, checking your address against flood databases.
- Comparing our records with third parties, like Lexis Nexis, to assess how valid the data is.
- Sharing with other insurers, price comparison websites, re-insurers, brokers and other third parties who help us to deal with your policy or product.
- Sharing with carefully chosen partners to add value to our products.
- Sharing data with providers of stand-alone AI applications that help us, or with third parties who provide services that use AI elements.

How long we keep your data

We only hold onto your personal data for as long as it's needed to either supply you with your Admiral policy or product, or for legitimate business purposes.

How long we keep hold of your personal data depends on why we're using it. Get in touch if you have any questions about our data retention policy.

To keep things simple, here are short summaries of our different 'retention periods', and how we decide what they'll be:

Data that's kept until you ask us to remove it

It's your right to ask us to delete certain bits of your personal data.

Find out more about your right to delete it, and when we can remove it.

Data that expires after a specific time period

We set time limits so some data is automatically removed after a certain period of time. How long we keep it is different depending on what type of data it is, and what we need it for.

For example, we usually keep policy records for seven years after the end of our relationship with you. But this could be longer if there are any claims that haven't been sorted, or if there's another legitimate reason for us to keep them.

Data that's kept for extended time periods for limited purposes

After your policy or product comes to an end, we keep some data for longer - but only for very limited reasons. For example, there might be legal or contractual reasons we have to hold onto it.

This could include:

- data retention laws
- official requests from the government to hold onto information for an investigation
- keeping data that might be needed for legal proceedings

Transferring data to other countries

We might share your personal information with other companies in the Admiral Group, or trusted service providers based outside the UK and the European Economic Area (EEA).

This usually happens when we store data in cloud systems. We aim to keep your data within the UK and EEA, but sometimes overseas providers might need to access it. For example, to help with technical support or troubleshooting.

Sometimes, the data protection laws of these countries aren't as comprehensive as the laws in the UK or EEA. If that's the case, our priority is to make sure your data is kept as safe as possible. Whenever we transfer data internationally, we use tools to:

- make sure the data transfer complies with any laws that apply
- help give your data a suitable level of protection

To make sure each data transfer complies with any laws that apply, we use these legal safeguards:

Standard Contractual Clauses ('SCCs')

These clauses mean the other party has to protect your data and provide you with a certain level of rights and protections.

For example, we use SCCs with the equivalent UK clauses (IDTA) to transfer your personal data.

You can exercise your rights under the SCCs, or the IDTA, by getting in touch with us.

Adequacy decisions

Adequacy decisions mean we can transfer personal data between the UK and the EEA.

We can also transfer personal data to certain other countries outside of the EEA that have adequate laws to protect personal data - this is decided by the European Commission and UK government. For example, we might transfer your personal data to our shared service centres based in Canada.

We also use some extra protections, depending on what's right for each data transfer. For example:

- technical protections, like encryption and pseudonymisation (in a nutshell, this is when we replace any data that could identify you personally with placeholder values, for increased protection)
- policies and processes to challenge disproportionate or unlawful government authority requests

If you have any questions or concerns about how we transfer your personal data, don't hesitate to get in touch.

Keeping your personal data safe

Our cyber security commitment

We care about looking after your personal information. And we understand how important it is for you to feel confident when you're using our website and services.

To make sure we keep your data safe, we've introduced some really robust risk management standards.

How we look after your data

Our information security measures

When you use our online services, we work hard to protect your information using some industry standard security practises.

We use encryption protocols to protect all the sensitive data that's transmitted to our servers.

Secure transactions and connections

When you get a quote or make a transaction on our website, all the data is processed on our secure servers using encryption technology.

You can tell you've got a secure connection in your browser if you see the padlock symbol.

Empowering you to stay secure

Your User ID and password are key to keeping your information safe, so please keep them safe and never share your password.

If you find out your account information has been exposed, change your password straight away and turn on multi-factor authentication.

If you ever think your credit card information has been compromised, get in touch with your card provider straight away. After you get your new card, let us know and we'll update your information.

Got any worries about your Admiral account? Don't hesitate to get in touch and we'll be on hand to help!

How you can look after your data

Responsible communication and cyber hygiene

We always do everything we can to keep your data safe. But there's lots you can do to protect yourself too!

Cybercriminals could try to trick you into sharing sensitive details by pretending to be a trusted contact or organisation.

Here are some helpful tips to help you spot phishing emails:

- Check the sender's email address for any mistakes or misspellings.
- Watch out for emails that are unexpected, unusual or ask you to share any confidential or payment information.
- Be wary of emails that try to encourage you to take urgent action or manipulate your emotions to act without checking.
- Be wary of emails that use a generic greeting.
- Hover your mouse over links to verify where they're going before clicking.

- Never download attachments from unknown or suspicious sources.
- If an email appears to come from a colleague or organisation but something feels off, check if it's authentic through a separate channel before responding.

When you need to send sensitive information by email, always use encrypted messaging services or secure file transfer platforms whenever possible.

Avoid including confidential data in the body of an email unless you're certain the connection is secure, and you can trust the recipient.

Want to know more? Find out more about how to protect yourself from insurance scams and fraud.

If you've been the victim of fraud or have any suspicions about an email or call that's claiming to be from us, get in touch with us directly.

Dealing with other people

All policies will have a policy administrator. Essentially, they're the person who handles the policy's paperwork and payments, and who we'll speak to when it comes to managing it!

The policy administrator:

- will have access to all the documents, information and personal data relating to anyone who's insured on the policy
- can choose another policyholder to become the policy administrator
- can make any changes to all parts of the policy
- can cancel the policy (in line with General Condition 4 of your policy book)

Apart from when it comes to cancelling your policy, our rule is to only deal with people named on your policy or any 'acceptable callers'. An acceptable caller is:

- a policyholder
- a named driver
- the spouse, partner or parent of a policyholder
- a secretary or personal assistant who's been added by a policyholder
- any other person, or organisation, that can show evidence they have the authority to act on the policyholder's behalf, and passes our data protection procedure

If you'd like someone else to regularly deal with your policy on your behalf, feel free to let us know by:

- Contacting us online
- writing to us at Admiral Group plc, Ty Admiral, David Street, Cardiff, CF10 2EH

For more information, see the terms and conditions for the relevant product or policy.

Marketing

Our companies across the Admiral Group have lots on offer. And from time to time, we'd like to keep you in the loop on any news or product updates from them.

That might be other insurance, legal or financial products, or some offers or promotions we think you might find interesting. We might share them by telephone, post, email, social media channels or text.

If you've visited our site and asked about one of our services, we might call you or get in touch another way to discuss what cover options we have for you.

We also advertise online on our quote journeys and in MyAccount. These ads can be personalised to keep you up to date on our promotions, what we're up to, and to help you find our services.

Like lots of companies, we show Admiral banners and ads that are targeted to you when you're on other websites and apps. We do this using a variety of digital marketing networks and ad exchanges.

We use a range of advertising technologies, like web beacons, pixels, ad tags, cookies, and mobile identifiers. We also use more specific services offered by some sites and social networks, like Facebook's Custom Audience service.

See our cookie policy for more information about this advertising, and how to exercise your rights.

Getting in touch or opting out

We'll give you the option to opt out of our marketing, firstly when you buy or get a quote for something from us, and whenever we send you any marketing.

You can get in touch if:

- you'd rather we didn't contact you with marketing
- you want to let us know how you'd prefer to be contacted (for example, by email or by post)
- you'd like to confirm the types of products and services that most interest you

To do that, you can:

1. Email us at marketingpreferences@admiralgroup.co.uk
2. Write to us at: Data Protection Officer, Ty Admiral, David Street, Cardiff, CF10 2AA

Artificial intelligence

Artificial intelligence (AI) is a way of teaching machines to do things that usually need human thinking. For example, spotting patterns in data, making predictions or creating new content.

We use AI to support our existing activities, including processing your personal data.

Before we process your personal data using AI, we do risk assessments and review the AI use cases to make sure our use complies with data protection laws, the Equality Act 2010, and other regulatory standards.

Just so you're aware, we use some external companies to give us certain AI applications. We might share your personal data with those other companies so we can use those applications. Find out more about how we share your personal data.

We mostly use AI for:

- underwriting and pricing (for example, improving our pricing models and using collected data to give people an accurate price for insurance or other finance products)
- managing claims
- helping find and stop fraud
- customer communications, experience, and engagement (for example, we offer virtual AI chatbots to help you, use AI in marketing to recommend relevant content, and to improve certain processes, like speeding up how long it takes us to process a complaint)

Automated decision making

We use some automated processes to make decisions.

These processes use data that you've given us, other records we have access to, and data from other companies to find out more about the personal data we collect to make some predictions. These include:

- how likely you are to make a claim, and how much it might cost
- how likely you are to buy a product
- the potential for fraudulent claims

This helps us decide which products are right for you, the terms of our agreement, how much it might cost, and any premium finance options.

To get you the right price for your product, we take these steps:

1. Collecting your data: We identify you, and you let us know what product you want to apply for (for example, whether you'd like insurance or a loan).
2. Validating your data: When we get your data, we do some checks to verify the information (for instance, confirming your identity) and add some third-party information, too (find out more about what personal data we collect).
3. Working out your price: We use data and statistical methods to work out how likely it is that you might make a claim or miss a payment, and what that could cost. This assessment includes things like local crime rates, repair costs, and credit history. For example, if you live in an area with lots of car crime, the cost of your insurance might be more.
4. Offering you a product: After checking your product 'risk', we work out if our product is right for you and your circumstances. If it is, we'll give you a final price including details of any commission and insurance premium tax, if it applies.

Your personalised price might be sent to you through some marketing channels, including from price comparison websites or third-party partners that you have a relationship with.

We also use automated decisions throughout your policy, like when we're offering you a renewal price or processing a claim.

If an automated decision might have a legal or other significant impact, it's your right to ask us to explain the logic behind these decisions.

For example, we have a dedicated Pricing Queries team to help explain the reasoning behind our price calculations. Find out how to get in touch with us.

How to get in touch

Got a question?

If you have any questions about your rights, or think that they haven't been met by us or any of the companies within Admiral Group, please get in touch with our Data Protection Officer.

You can:
Send us an email at yourinformationrights@admiralgroup.co.uk

Write to us at:
Data Protection Officer
Admiral Group plc
Ty Admiral
David Street
Cardiff
CF10 2AA

Have a complaint about how we've processed your personal data?

If you have any complaints about how your personal data has been processed, and you're not satisfied with our response after you've escalated it to our Data Protection Officer, you also have the right to complain to the relevant Data Protection Regulator.

In the UK, this is the Information Commissioner's Office (ICO). You can contact them at:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

AD-PP-001