



# Your Privacy and Security

## Introduction

This privacy policy will help you understand how we collect, use and protect your personal data. You should also show this notice to anyone else whose details you provide to us, such as the owner of the vehicle or any additional drivers.

**You acknowledge that by providing your personal data to us, you consent to its processing in the manners outlined below. When providing personal data about others, you confirm that you have the consent of these individuals to supply their personal data. We are unable to offer you any product or service unless you provide explicit consent for the collection and use of sensitive personal data as defined in the Data Protection Act 1998.**

## Who we are

Veygo is a trading name of the data controller EUI Limited (Registered Number 02686904). EUI Limited is part of Admiral Group plc.

Companies within Admiral Group plc:

- **EUI Limited;** trading as Admiral, Bell, Diamond, Veygo and Elephan
- **Able Insurance Services Limited;** trading as Gladiator
- **Admiral Law Limited;** trading as Admiral Law
- **BDE Law Limited;** trading as EUI Law, Diamond Law and Elephant Law
- **Inspop.com Limited;** trading as Confused.com

We use the following data processors to assist in your application for, and active membership of the Veygo platform; this includes the purchase of insurance products, communication with other members, and the use of the rental services Veygo provides:

- **Stripe Payment Europe Limited** for processing payments. To view their privacy statement please [click here](#).
- **PayPal (Europe) Limited** for processing payments. To view their privacy statement place [click here](#)

At all times, EUI Limited will remain the data controller.

## Data we collect

We collect **personal data** and **sensitive personal data** as part of providing services to you.

**We may also monitor or record calls, emails, SMS messages or other communications in accordance with UK law.**

**We may collect your Driving Licence Number (DLN or “MyLicence”) as part of your application for car sharing insurance (in some cases, we may not be able to insure you without this information) or when you make a claim.** For details relating to information held about you by the Driver and Vehicle Licensing Agency (“DVLA”) please visit [www.dvla.gov.uk](http://www.dvla.gov.uk) and [www.myllicence.org.uk](http://www.myllicence.org.uk)

To view your driving licence, visit [www.gov.uk/view-driving-licence](http://www.gov.uk/view-driving-licence).

## Types of data we may collect

### PERSONAL DATA

Examples of personal data we may collect include:

- Name and address, date of birth and gender
- Telephone numbers and email address
- Employment status
- Credit/debit card details
- Lifestyle and other information

### SENSITIVE PERSONAL DATA

Examples of sensitive personal data we may collect includes:

- Medical history
- Claims history
- Criminal convictions etc.

### DRIVING LICENCE NUMBER (“MYLICENCE”)

The number is used to do an automatic check with the DVLA driver database, to retrieve the required information. The provided information is:

- Type of licence held
- Length of time the licence has been held for
- Entitlements to drive
- Penalty points
- Convictions
- Conviction dates
- Disqualifications

## CALL RECORDING AND MONITORING

We monitor or record calls, emails, SMS messages or other communications for:

- Business purposes such as quality control and training
- Processing necessary for entering into or performance of a contract
- Prevention of unauthorised use of our telecommunication systems and websites
- Ensuring effective systems operation
- Meeting any legal obligation
- Protecting your vital interests
- Prevention or detection of crime
- For the legitimate interests of the data controller

## When data is collected

**We will collect your personal data when:**

- You ask for a quote
- You purchase our products and services
- You make a booking request
- You verify and complete your profile
- You make customer enquiries
- You register for information or other services
- You register a claim
- You respond to communications or surveys
- We require additional information from you for validation purposes

## How your data is used

**We will use your data for:**

- Processing your quotes
- Processing your booking requests
- Administering your policy, including claims handling
- Fraud prevention and detection
- Credit scoring or other automated decision-making systems
- Administering debt recoveries
- Verifying your identity when required
- Undertaking market research, product development and statistical purposes
- Keeping you informed about promotions and new developments by email, telephone or post
- For assessment and analysis to enable us to review, develop and improve the services which we offer and to enable us to provide you and other customers with relevant information through our marketing programme.
- We may use your information to make decisions about you using computerised technology to profile you, such as assessing which products might be most suitable for you.

## Driving Licence Number (“MyLicence”)

The data provided by the DVLA may be used alongside other information you have provided:

- To calculate a motor insurance quote
- To administer the policy
- For anti-fraud purposes

**They will not be used for any other purpose, or be made available for anyone else.** Only the motor insurance industry may use this information. If you apply for a quote with us, or membership of the platform and don't decide to take out insurance with us or complete your registration, the data returned from the DVLA database will be anonymised or deleted no later than 30 days after receipt of that data.

**Please note that under our User Agreement with the Motor Insurance Bureau, individual agents do not have access to the data returned by a DLN search and as such will not be able to discuss issues relating to your DLN with you.** In these instances, we suggest checking the information associated with your DLN is correct at [www.gov.uk/view-driving-licence](http://www.gov.uk/view-driving-licence).

## Dealing with other people

**With the exception of cancellation (General Condition 4), it is our policy to deal with any acceptable callers.**

An acceptable caller is:

- the spouse, partner or parent of a Policyholder
- any other person or organisation that provides evidence that they have authority to act on behalf of the Policyholder and passes our data protection procedure

If you would like someone else to deal with your policy on your behalf on a regular basis please let us know.

## Claim process

**To ensure an efficient and speedy claim process we will take instruction from you or from any other person you have confirmed as an acceptable caller.** If you would like someone else to deal with your claim on your behalf please let us know.

**If you give us data about another person, in doing so you confirm that they have given you permission to provide it to us to be able to process their personal data** (including any sensitive personal data) and also that you have told them who we are and what we will use their data for, as set out in this policy.

## Marketing

Admiral Group plc will contact you from time to time by telephone, post, email, social media channels or SMS to keep you informed with news, our range of products or services.

### MARKETING & YOUR PREFERENCES

**Admiral Group plc has various offerings from time to time we would like to keep you informed of news, products or services**, including but not limited to insurance (e.g. other automotive, insurance, legal or financial products, or other carefully selected offers or promotions which we feel may be of interest to you).

**If you have visited our site and have selected to view a quote, we may contact you**, by telephone or other means, to discuss your quote and the cover options available to you.

**Other carefully selected companies may also contact you** by post. If you have opted in to receive emails, SMS or telephone calls from other selected companies, you may also be contacted about other products that we believe may be of interest to you by these contact methods.

**If you would like to alter your marketing preferences** please [click here](#) or write to the Marketing Department, EUI Limited, Tŷ Admiral, David Street, Cardiff, CF10 2EH.

## Our technology

We collect data about you through the use of technology such as cookies and device fingerprinting. [Click here to view our full Cookie Policy.](#)

### YOUR COOKIE PREFERENCES

#### Managing, Disabling And Enabling Cookies

You have the ability to accept or decline cookies from any website by modifying the settings in your browser. If you wish to restrict or block the cookies which are set by our website, you can do this through your browser settings. For information about how to manage and disable cookies you can use the 'Help' function within your browser or please visit [www.aboutcookies.org](http://www.aboutcookies.org) or [www.allaboutcookies.org](http://www.allaboutcookies.org). However, please note that by deleting or disabling cookies this could affect the functionality of our website and you may not be able to access certain areas or features of our site.

To opt out of being tracked by Google Analytics across all websites [click here](#).

## Who has access to your data

Apart from ourselves, other companies that may have access to your data include:

- **Companies within the Admiral Group** (For the purposes of this Privacy Statement, “Admiral Group” means Admiral Group plc and any company or entity in which Admiral Group plc owns more than 15% of the issued share capital. Companies in the Admiral Group shall include, without limitation, EUI Limited, Admiral Insurance Company Ltd, Admiral Insurance (Gibraltar) Ltd, Inspop.com Ltd, Able Insurance Services Ltd and any other company that is incorporated within the Admiral Group at any time in the future). A full list of our companies can be found at [www.admiralgroup.co.uk/business/our\\_companies.php](http://www.admiralgroup.co.uk/business/our_companies.php)
- **In the event that we undergo re-organisation or are sold to a third party**, in which case you agree that any personal data we hold about you may be transferred to that re-organised entity or third party.
- **Where it is necessary to deliver the products and services bought by you.** For example, we may disclose your personal data to Theodo UK who host any data collected from this website and to Stripe Payment Europe Limited and Paypal (Europe) who process payments on our behalf. It may also be necessary for us to pass your personal data to the organisation from whom you have ordered any products or services other than your EUI Limited insurance product, such as a travel insurance or a personal accident cover provider, etc. At all times, EUI Limited will remain the data controller unless we inform you otherwise.

## Request your data

You have the right to access the data we hold about you under Section 7 of the Data Protection Act 1998.

### HOW TO MAKE A SUBJECT ACCESS REQUEST

**Please write to:**

Head of Central Quality  
Subject Access Request  
EUI Limited  
Tÿ Admiral  
David Street  
Cardiff CF10 2AA

**Please provide:**

1. Your name, address, policy/claim number and what information you would like.
2. Identification documents; one which shows your name and signature (e.g. a copy of your passport) and one which shows your name and address (e.g. a copy of a recent bill or bank statement or other official document).

We will accept just one identification document if it shows your name, address and signature such as a copy of your driving licence. (This is to take reasonable steps to confirm your identity before providing you with details of any personal information we may hold about you.)

3. A cheque or postal order made payable to “EUI Limited” for £10.00 (In accordance with the Data Protection Act 1998, we are entitled to charge a fee of £10.00 to cover the administration costs.)

Please note that if your SAR involves personal data of other people or you are making a request on behalf of another (such as a parent on behalf of their child), we may need identification from these individuals, as well as a signed letter of authority from them confirming that they are happy for you to act on their behalf and for us to release their data to you.

Once we have received your written request, identification documents and fee we will have 40 calendar days to fulfil your request.

## Confidentiality and disclosure of your data

We will endeavour to treat your personal data as private and confidential. From time to time we will employ agents and subcontractors to process your personal data on our behalf. The same duty of confidentiality and security will apply to them and all processing will be carried out under our instruction.

**We would like to bring to your attention our obligations to disclose data in the following four exceptional cases permitted by law, and the other situations set out below.** These are:

- Where we are legally compelled to do so
- Where there is a duty to the public to disclose
- Where disclosure is required to protect our interest
- Where disclosure is made at your request or with your consent
- **In the unfortunate event that you have to make a claim then we will need to disclose data with any other party involved in that claim.** This may include:
  - Third parties involved with the claim, their insurer, solicitor or representative
  - Medical teams, the police or other investigators

If you make a complaint about the service we have provided, we may be obliged to forward details about your complaint, including your personal data, to the relevant ombudsman. You can be assured that they are similarly obliged to adhere to the Data Protection Act and keep your personal data strictly confidential.

**Please note that we make a number of checks verifying identities to prevent and detect crime and money laundering, as well as data sharing at any time for the purposes of fraud prevention. These checks may also include your DLN/MyLicence.**

Using data obtained from your DLN, we may pass details of your 'No Claims Bonus' to certain organisations to be recorded on an NCB database. This may occur if information requires updating or correcting at any stage, and also at the renewal stage of your policy and upon or after the cancellation of your policy prior to the expiry date.

## Use of your data for fraud prevention & detection and credit checking

### CREDIT REFERENCE

When you apply to us to open an account, we make a number of checks to assess your application for credit and verifying identities to prevent and detect crime and money laundering. To obtain this information, we will check the following records about you and anyone else who may also be insured and whose personal details have been provided as part of the insurance application.

- Our own records.
- Credit Reference Agency (CRA) records. When we search these records CRAs will place a search footprint on your credit file that may be seen by other lenders. They supply us with 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 will supply us with information, including the Electoral Register and credit information. The agencies will record details of the search whether or not your application proceeds. **The searches will not be seen or used by lenders to assess your ability to obtain credit.** We may use scoring methods to assess this application and to verify your identity.

Credit searches and other information which is provided to us and/or the credit reference agencies, about you and those with whom you are linked financially, may be used by EUI Limited and other companies if you, or other members of your household, apply for other facilities including insurance applications and claims. This information may also be used for debt tracing and the prevention of money laundering as well as the management of your account. Alternatively, we may ask you to provide physical forms of identification.

We may also make periodic searches at CRAs and FPAs to manage your account with us.

Information on applications will be sent to and recorded by CRAs. When you borrow from us, we will give details of your account(s) and how you manage it/them to CRAs. If you borrow and do not repay in full and on time, CRAs will record the outstanding debt. This information may be supplied to other organisations by CRAs and FPAs to perform similar checks, and to trace your whereabouts and recover debts that you owe. Records remain on file for six years after they are closed, whether settled by you or defaulted.

If you give us false or inaccurate information and we suspect or identify fraud, we will record it and may also pass this information to FPAs and other organisations involved in the prevention of crime and fraud.

If you borrow from us and do not make payments that you owe us, we will trace your whereabouts and recover debts.

Your data may also be used for other purposes for which you give your specific permission or, in very limited circumstances, when required by law or where permitted under the terms of the Data Protection Act 1998.

## HOW TO FIND OUT MORE

This is a condensed guide to the use of your personal information for credit referencing. If you would like to read the full details of how your data may be used please phone our Customer Services Department, or write to us at Pricing Department, Ty Admiral, David Street, Cardiff, CF10 2AA.

You can contact the CRAs currently operating in the UK; the information they hold may not be the same so it is worth contacting them all. They will charge you a small statutory fee.

Call Credit - [www.callcredit.co.uk](http://www.callcredit.co.uk)

Equifax - [www.equifax.co.uk](http://www.equifax.co.uk)

Experian - [www.experian.co.uk](http://www.experian.co.uk)

## WHEN YOU MAKE A CLAIM

If necessary we may also have to investigate your claims and conviction history in the course of administering the claim. You can be assured that we will keep such investigations strictly confidential.

We pass information to the Claims Underwriting and Exchange Register, run by Insurance Database Services (IDS) and, in the case of motor insurance, the Motor Insurance Anti-Fraud and Theft Register, run by the Association of British Insurers (ABI). This helps insurers check information and prevent fraudulent claims. When we deal with your request for insurance we may search these registers. Under the conditions of your policy, you must tell us about any incident (such as an accident or theft) which may give rise to a claim. When you tell us about an incident we will pass information to the Registers.

Information relating to your insurance policy will be added to the Motor Insurance Database ("MID") managed by the Motor Insurers' Bureau ("MIB"). MID and the data stored on it may be used by certain statutory and/or authorised bodies including the Police, the DVLA, the DVANI, the Insurance Fraud Bureau and other bodies permitted by law for purposes not limited to but including:

- Electronic Licensing
- Continuous Insurance Enforcement; Law enforcement (prevention, detection, apprehension and or prosecution of offenders)
- The provision of government services and or other services aimed at reducing the level and incidence of uninsured driving

If you are 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 obtain relevant information.

Persons (including his or her appointed representatives) pursuing a claim in respect of a road traffic accident (including citizens of other countries) may also obtain relevant information which is held on the MID.

It is vital that the MID holds your correct registration number. If it is incorrectly shown on the MID you are at risk of having your vehicle seized by the Police. You can check that your correct registration number details are shown on the MID at [www.askmid.com](http://www.askmid.com).

## **FRAUD PREVENTION AND DETECTION**

In order to prevent and detect fraud insurers may, at any time share information about you with our other group companies.

If false or inaccurate information is provided and fraud is identified details will be passed to fraud prevention agencies. Law enforcement agencies may access and use this information.

We and other organisations may also access and use this information to prevent fraud and money laundering, for example, when:

- checking details on applications for credit and credit related or other facilities
- managing credit and credit related accounts or facilities
- recovering debt
- checking details on proposals and claims for all types of Insurance
- checking details of job applicants and employees

## **MYLICENCE**

As part of our fraud prevention and detection measures, we may undertake searches against your (or any person included on the proposal) DLN against details held by the DVLA to confirm your licence status, entitlement and restriction information and endorsement/conviction data. This helps insurers check information to prevent fraud and reduce incidences of negligent misrepresentation and non-disclosure. A search of the DLN with the DVLA should not show a footprint against your (or another relevant person included on the proposal) driving licence.

Please contact us on 0800 052 3144 if you want to receive details of the relevant fraud prevention agencies.

We may exchange your details such as NCB, DLN and Claims records with insurance industry databases for the purpose of validation and financial crime prevention.

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

## Information Security

**On our websites we protect any data you have given us by providing you with a User ID and password.** We also use industry standard security to encrypt sensitive data in transit to our servers.

**It will be necessary to transfer your personal data to other Group companies or service providers located outside of the European Economic Area.** The data protection and other laws of these countries may not be as comprehensive as those in the UK or the EEA - in these instances we will take steps to ensure that your data is given an equivalent level of protection as it is in the EEA.

If you have entered your credit card information on what you think might be a malicious website or replied to an e-mail with that information, you should contact your credit card company immediately. Do not forget to contact us to update your card details.

When you ask for a quote from us, we will process the data on a secure server. Your browser will confirm that you are in a secure area by displaying an unbroken key or lock in the bottom right hand corner of your browser window.

Many organisations use security features such as firewalls to protect their computer systems. These firewalls may prevent you from connecting to our secure server to get a quote. If you are at work and cannot connect to our web site, please speak to your IT administrator.

Please be aware that communications over the Internet, such as emails, are not secure unless they have been encrypted. Your communications may route through a number of countries before being delivered - this is the nature of the Internet. We cannot accept responsibility for any unauthorised access or loss of personal information that is beyond our control.

Additionally, you can protect your system by installing anti-virus and running scans as recommended by the vendor. You should also run any security updates / patches you receive for your system from the supplier.

Never respond to unsolicited emails from unfamiliar sources. Such emails may be fraudulent and attempt to get you to provide your personal details or payment information.

## Changes to this policy

**This privacy policy was last updated on 12 October 2017.** We reserve the right to make changes to this policy and you will be prompted of any changes when you next visit our website.

**From time to time we may need to change the way we use your personal data.** Where we believe you may not reasonably expect such a change we will write to you. When we do so, you will have 60 days to object to the change but if we do not hear from you within that time you consent to that change.