Using my personal data – Motor Products

Full Privacy Notice

Introduction

When you apply for, use our website or purchase insurance with First Central Insurance Management Limited, we ask you to review our online privacy notice, which gives summary information about how we use your personal data. In this notice, “we”, “us” and “our” mean First Central Insurance Management Limited and First Central Underwriting Limited, unless we say otherwise. This full notice gives you additional information about how we use your personal data to provide our services.

Contents

1. Who are you giving your information to?

There are two **controllers** who collect and **process** your **personal data** when you interact with or purchase our insurance product:

First Central Insurance Management Limited

They're the insurance intermediary and provider of the finance product. They handle the day-to-day administration of your policy, claims and finance. They're your main point of contact for any data protection-related requests you may have.
They're registered as a controller with the UK Information Commissioners Office under certificate number Z1389426**.**
Registered Address:
Capital House, 1-5 Perrymount Road, Haywards Heath, West Sussex, RH16 3SY
Contact the Data Protection Officer at DPO@1stcentral.co.uk.

First Central Underwriting Limited

They're the insurance provider and underwrite your insurance policy. They assess and determine the terms of the policy and the associated premiums.
They're registered as a controller with the Gibraltar Information Commissioners Office under certificate number DP 009121.
Registered Address:
5.1a Waterport Place, 2 Europort Avenue, Gibraltar GX11 1AA
Contact the Data Protection Officer at DPO@1stcentral.co.uk.

The **controllers** will together or separately decide what **personal data** is collected, the **lawful basis** for **processing**, how that **personal data** may be shared and how long it will be kept.

This notice applies to all our motor insurance products. The processing activities described in this notice reflect the range of ways we may use personal data across our products, services, and brands (including trading names such as Picnic and Motivo). Processing is described at a general level and may vary depending on the product and the individual's specific service experience.

Where a section only applies to a particular product, such as 1st Central Connect, we have made this clear in that section.

2. What information do we collect?

We collect the following types of **personal data** about you:

Basic Personal information

- Full name and title
- Full address and postcode
- Date of birth
- Marital status
- Gender
- Employment status and Occupation
- Telephone number
- Email address
- Driving License Number
- Vehicle registration, make and model, modifications
- Claims history
- Residency
- Home ownership
- Accident location and details
- No Claims Discount
- Driving Behaviour (1st Central Connect only)
- Demographic such as lifestyle, income, and education

Sensitive personal information

- Personal injury from previous claims
- Medical conditions that affect your license
- Motoring **convictions,** dates, and type
- Information pertaining to vulnerability

Payment information

- Card number, expiry date and CSV
- Bank account number and sort code

Electronic Identifiers

- IP address, device ID
- Mobile device ID
- Mobile app usage

Information you give to us on behalf of others

- Named driver – full name, date of birth, employment status, license numbers and **conviction** information
- Payers – the payment information, names, address, and email if someone else is paying
- Relatives or authorised representatives – full name and date of birth
- Third Party – if involved in a claim including name, vehicle registration
- Passengers – if involved in a claim

Information we receive from others

- Credit score, default Information, county court judgements/IVAs and financial history
- Identity fraud markers
- No Claims Discount and driving entitlements
- Additional mobile application and device Information
- Locational and Sensor information (1st Central Connect only)
- Vehicle MOT and Tax history

3. How will we use your information?

If you're considering buying, or have bought, a motor product, we'll use **personal data** to carry out the activities described below. We won't use your data in ways you would not reasonably expect or in ways that have unjustified effects. We have set out the **lawful basis** for using **personal data** and, where relevant, the additional condition we rely on for **special category data** or **criminal conviction data**. Where we rely on legitimate interests, we balance those interests against your rights and freedoms.

Activity	Description	Reason for Activity
Providing you a quote for insurance	Whether you come directly to us or through a price comparison website or other provider we will capture and process **personal data** to evaluate the insurance risk and provide a quote for insurance. We undertake this activity through **modelling,** using internal and external sources of data and the decision is made by **solely automated means** that include **profiling**. See section 8 for more information. This can include **sensitive personal data.**	Necessary for entering and performance of a Contract. Substantial Public Interest – Insurance Purposes
Providing you a quote for finance	We will process **personal data** to assess options for how you can pay for the insurance product e.g.by finance or paying in full. We conduct credit and affordability assessments that will determine your suitability for our finance product and on what terms this can be provided. We undertake this activity through **modelling** using internal and external data and the decision is made by **solely automated means** that include **profiling**. See section 8 for more information. This will not include **sensitive personal data**.	Necessary for entering and performance of a Contract. Regulatory Obligations - with respect to consumer credit and ensuring affordability
Validating your identity at quote and sale	We will validate your identity using the **personal data** you provide at quote and following sale. We are obligated to complete customer due diligence, to reduce the risk of fraudulent policies being purchased. We use public data such as the electoral role and data sourced from credit reference agencies and insurance databases for this purpose. Discrepancies in **personal data** can lead to insurance becoming invalid. If we identify this post sale, we will contact you and request that you provide certain documentation to help us validate your identity, this could include copies of: - Drivers Licenses - Passports or other Identity Documents This can include **sensitive personal data**.	Legitimate Interest in meeting regulatory requirements related to knowing our customer Legitimate interest in preventing and detecting fraud and ensuring accuracy in our decision making. Substantial Public Interest – Insurance Purposes Substantial Public Interest – prevention and detection of unlawful acts
Accepting payment of deposit and future payments	If you decide to purchase a product, we'll need to process **personal data** to collect the deposit, full payment or set up direct debits. *Paying Online or Telephone – Deposits and in Full*: Our website meets Payment Card Industry standard for the safe capture of the payment information and for sending it to the payment gateway for your banking provider. We also	Legitimate interest in preventing and detecting fraud and ensuring accuracy in our decision making.

	provide a telephony system for you to enter your details offline. Your payment card information is not recorded in our calls, and our colleagues do not have access to it. *Paying Monthly*: If you want to pay monthly by direct debits or by payment card using Continuous Card Authority (CCA) we'll capture your bank instructions/payment card data. We use a banking validation service to ensure the accuracy of the bank account information we're given. Please refer to our policy wording and credit agreement for more information about CCA and your rights. We will retain the payment card for the duration of your policy to support you in future transactions, at renewal, to prevent fraud and to ensure that any refunds which become payable can be returned. You can request a payment card is removed. If you use a third party to pay, we will collect their name, email and address to use in communications about the payments. This will not include **sensitive personal data**.	Payment is necessary for entering and performance of the Insurance Contract. Legal Obligation - Prevention of money laundering Payment by direct debit or CCA is necessary for entering and performance of the Credit Agreement. Legitimate Interest in performing automatic renewals, performing refunds and Mid Term transactions.
Providing you insurance cover and service	We need to process **personal data** for the administration of your policy including: ▪ Setting up and recording your policy ▪ Cancellation and/or renewal of your policy ▪ Performing midterm adjustments ▪ Providing customer care through email, social media, web chat, and telephone ▪ Handling any issues, concerns, or complaints ▪ Providing access to other policy benefits and services This can include **sensitive personal data**.	Necessary for entering and performance of a Contract. Substantial Public Interest – Insurance Purposes.
Validating your insurance cover	We will process your **personal data** to validate the accuracy of your insurance. This means we will check any data you provide against existing internal data we hold and external sources of data to ensure the information is accurate and that your insurance is valid. This can include validating: - Your driving license, driving history, and convictions - Vehicle MOT and servicing - Occupation and vehicle use - Your No Claims Discount status This can include **sensitive personal data**.	Legitimate interest in ensuring you have valid insurance cover, and we are covering the correct risk. Substantial Public Interest – Insurance Purposes. Substantial Public Interest – prevention and detection of unlawful acts.
Providing ancillary products	If you purchase an ancillary product, we will share your **personal data** with the insurer and intermediaries for those products to enable them to provide their services. See section 4.5 for more information on Ancillary Partners. Please note they are **controllers** for this purpose. We recommend you review their privacy notices which are available in the applicable ancillary policy wording for the product you are buying. This can include **sensitive personal data.**	Necessary for entering and performance of a Contract. Substantial Public Interest – Insurance Purposes.
Managing vulnerabilities	If you tell us about a vulnerability, or we identify one through our analysis, we will record relevant details and use them to support you.	Legitimate Interest for meeting regulatory obligations.

	We monitor and analyse how vulnerable customers are treated to help ensure fair outcomes. Where relevant, we may share vulnerability information with service providers, such as a debt recovery provider, so they can take it into account when supporting you. This can include **sensitive personal data**.	Substantial Public Interest – Safeguarding Economic Interest.
Updating Industry Databases	We're required to notify the Motor Insurance Database ("MID") when insurance is purchased and the Claims Underwriting Exchange ("CUE") or Motor Insurance Anti-Fraud and Theft Register ("MIAFTR") of any claim activity. We may need to share this information with law enforcement. See section 4 of this notice for more information about these databases. This can include **sensitive personal data.**	Legal Obligations – under the Road Traffic Act and Insurance Directives Legitimate Interest – protecting the wider insurance industry and improving accuracy of data. Substantial Public Interest – Insurance Purposes.
Claim handling	When you make a claim against your insurance, we will need to process the **personal data** and may need to collect additional information to provide the services. Claim handling can include: ▪ Setting up and administering any claims ▪ Deploying providers to recover, repair or retain your vehicle ▪ Dealing with any legal claims from third parties ▪ Providing you support for legal claims you may have ▪ Instructing medical experts or medical services ▪ Collation of evidence such as CCTV footage, images, reports, witness statements ▪ Managing reinsurance ▪ Settling any financial matters that arise from the claim. This can include **sensitive personal data.**	Necessary for entering and performance of a Contract. Substantial Public Interest – Insurance Purposes. Legitimate Interest – recovery of monies that are payable due to the claim.
Debt and claims debt recovery	If we need to recover any money from you in respect of missed payments or money due to a claim, we'll pass your **personal data** to a debt recovery service: This activity includes: ▪ contacting you to discuss payment arrangements ▪ setting up payment plans ▪ sharing information with credit referencing agencies ▪ progressing legal action We'll conduct legal recovery where necessary and will share **personal data** with our legal panel. This can include **sensitive personal data.**	Legitimate Interest – recovery of monies payable under the insurance or finance contracts. Legal claims
Fraud Analysis, Investigation, and Intelligence	We're committed to reducing insurance fraud for the benefit of our genuine customers and the insurance market. We are required to have a framework in place for managing fraud risk and this includes performing analysis, conducting investigations, gathering evidence, and undertaking intelligence activities. We balance fraud prevention with your privacy and assess fraud concerns case by case. We may not always be able to	Legitimate Interest – in the protection of you and us. Legitimate Interest – to meet regulatory requirements. Substantial Public Interest

	provide detailed transparency about these activities where doing so could prejudice fraud prevention, detection or investigation. ▪ We will use the **personal data** we have collected internally. ▪ We'll use external public and private sources of data such as government advisories, the national crime agencies, national fraud databases, social media platforms and other web sources when conducting these activities. ▪ We'll investigate all claims made to ensure they're legitimate, sharing concerns with other insurers, databases, investigators, and law enforcement where required. ▪ We use investigation services to support us in gathering evidence in our activities. ▪ We use **personal data** to profile individuals and fraud networks. ▪ We use automated processing to support these activities but do not make wholly automated decisions. ▪ We will support victims of insurance fraud. ▪ We'll retain fraud information if it's relevant and necessary. ▪ We use specially trained colleagues to handle these activities. This can include **sensitive personal data.**	– prevention and detection of unlawful acts. Substantial Public Interest – preventing fraud. Substantial Public Interest – preventing fraud (sharing with authorities).
Quality Assurance	We monitor the quality of our services, and we perform quality assurance activities. This includes: ▪ recording some of our telephone calls and monitoring their quality ▪ monitoring customer service through all communication channels ▪ considering any feedback, we receive from you after a transaction or claim ▪ considering feedback received from online review platforms ▪ considering any industry standards and benchmarking ▪ monitoring the suitability of our products and partners and how they are performing ▪ monitoring any complaints and root causes. This will not include **sensitive personal data.**	Legitimate Interest – product and service quality monitoring.
Service Communication	We will need to contact you regarding your insurance and our services. This will include updating you about your policy, your claim, and your finance. This can include letting you know about our opening hours, sending updated insurance documents, renewal invite reminders, payment reminders, updated contact details and changes to our services. All these communications will also be available in Your Account. We'll send service communications by email, post and SMS. These communications don't include promotional or marketing materials. This will not include **sensitive personal data.**	Legitimate Interest – keeping in contact with you about your insurance.

Marketing	We would like to send you promotional offers and details of new products. This includes where we run campaigns with partners. During your journey with us we will ask you to consent to this and you will be given an opportunity to provide us your preferences. Marketing can be sent by email, telephone, SMS, and post. You can opt out of this at any time with your preference centre in the customer portal and through unsubscribe links in our communications. We take reasonable steps to ensure that we don't contact individuals who are registered with the telephone preference service or are on public email or SMS suppression lists. We don't, under any circumstance sell our marketing records to third parties. This will not include **sensitive personal data**.	Consent
Personalisation	We want to tailor the experience you have with us through personalisation of our services. We consider this within any development or introduction of new functionality. Examples can include: ▪ pre-filling forms for ease of use in the customer portal ▪ tailoring what we show, and our rewards based on your products and needs ▪ remembering you on your account and welcoming you back ▪ this can include using artificial intelligence capabilities. This will not include **sensitive personal data**.	Legitimate Interest – customer journey and experience
Business Performance Administration	We monitor the performance of our business through our management information. These activities rarely require the use of direct **personal data** but may include reference to a claim or policy. We do this through Management Information ("MI"). We use MI to: ▪ track volumes of sales, renewal, transactions, claims ▪ consider our resourcing needs ▪ perform auditing of our finance and accounting ▪ manage issues ▪ make decisions about our products and services ▪ manage manual processes This can include **sensitive personal data.**	Legitimate Interest – management of our business
Legal or regulatory obligations	We may have to process your **personal data** to meet our legal or regulatory obligations. In most cases we can use anonymised information but on occasion we do have to provide **personal data**. ▪ court orders for disclosure ▪ financial or regulatory reporting ▪ dealing with regulatory or supervisory authorities ▪ law enforcement This can include **sensitive personal data,** but it's assessed case by case and depends on the nature of the requirement.	Legal Obligation Legitimate Interest – meeting regulatory requirements
Technologies	We use technologies which have artificial intelligence capabilities. This includes machine learning, robotics, and	Legitimate Interest

	speech analytics. These technologies are used to support activities in this notice. We have a framework for management and safeguarding the use of these technologies. See section 10. We include Cookies within this. Cookies allow us to track a user's journey, ensure security, and provide user functionality on our website. This can include **sensitive personal data**.	– in using technology to improve the processing Consent Preferences
Product Development and Innovation	We use **personal data** we've collected to help us improve or create new products and understand our customers. Where possible we use partly or fully anonymised data to conduct these activities. If we do have to use any **personal data**, we put in place additional safeguards identified through data protection impact assessments to mitigate any harm to you. We can use artificial intelligence capabilities to support this processing. We do not make any solely automated decisions with profiling about individuals as part of our development activities. These activities can include: ▪ Statistical analysis on our pricing and risk models ▪ Monitoring and improving our products ▪ Improving our customers journeys and functionality ▪ Understanding issues and root causes ▪ Benchmarking against the wider industry ▪ Enriching the data, we hold This could include inferred or indirect **special category data**. Where this happens, we will pseudonymise, aggregate or anonymise the data where possible to create new datasets.	Legitimate Interest - to improve and enhance our services and products Substantial Public Interest - archiving, research, and statistics (with a basis in law) specifically statistical analysis for insurance
Providing AI-assisted customer service and policy servicing	Where you interact with us through AI-assisted digital or telephone channels, we may process conversation information, policy/account information and interaction records to understand your enquiry, verify your identity, administer your policy and provide customer support. This may include using web-chat or phone-based bots for simple policy servicing tasks, such as routine questions, information checks and straightforward requests including policy cancellations. We may use transcripts, logs or service records to monitor quality, improve customer journeys, identify training needs and route requests to the right service. These activities do not involve solely automated decisions that produce legal or similarly significant effects.	Necessary for the performance of a contract. Legitimate Interest – improving customer service, quality assurance and operational efficiency.
What If I'm not a customer?		
I was a witness to an incident with your customer; how will you use my personal data?	We'll collect your **personal data to:** ▪ help us investigate, pursue, or defend a claim ▪ detect and prevent fraudulent claims ▪ communicate with you about a claim The **personal data** will be limited to basic contact information along with any statements you make. We might need to share your information with other insurers, legal representatives as part of this process. We'll retain your	Legitimate Interest – establishing or defending legal claims, meeting our regulatory obligations. Substantial Public Interest – prevention and detection of unlawful acts

	information on the claim. Our claim handlers will discuss with you the steps we need to take and what will happen. This could include **sensitive personal data.**	Substantial Public Interest – Insurance Purposes
I'm a third party on the claim; how will you use my personal data?	We'll collect your **personal data** to: ▪ To manage the claim ▪ Offer and provide services ▪ To validate identity ▪ To communicate about the claim ▪ To manage and resolve any concerns or complaints ▪ To detect and prevent fraudulent claims This notice is directly applicable to you. Please see who we share **personal data** with and the steps we take to prevent Fraud. This will include **sensitive personal data**.	Legitimate Interest – establishing or defending legal claims, meeting our regulatory obligations. Substantial Public Interest – prevention and detection of unlawful acts Substantial Public Interest – Insurance Purposes
I'm paying on someone's behalf; how will you use my data?	If you are paying for the insurance, the customer will be asked to provide us your name, postal and email addresses, payment, or bank account details, to perform the financial transactions. We will validate any banking information we receive. Whilst the responsibility will remain with the customer, we will send you communications confirming changes to payments, so you are also aware. You can request we remove your payment information. This will not include **sensitive personal data**.	Entering and performance of contract. Legitimate Interest – preventing and detecting fraud.

Sensitive Personal Data and Conviction Data

We may ask you to provide information that the law classifies as **special category data**, such as health information. We may also infer **special category data**, such as ethnicity, from residency or identity documents. We may also ask you to provide information about **criminal convictions** or alleged or actual criminal offences. We limit the collection of this information and restrict how it can be used.

Where we collect **special category data** or **criminal conviction data**, we process it where this is in the substantial public interest, including for insurance purposes, claim handling and the prevention and detection of unlawful acts relating to fraud.

We have a policy that governs how we use **special category data** and **criminal conviction data**. This information may be shared externally in limited circumstances where it is relevant to the activities described in this notice.

Children

We do not provide services directly to children and, therefore, do not need to capture their information. However, we may collect incidental information if it is relevant to a claim or is essential for assisting us in delivering services to vulnerable customers. We treat data relating to children the same as **sensitive personal data**. We'll discuss this with the parent or guardian of the child to ensure that everyone understands how that information will be used and shared.

Safeguarding our activities

We consider risks that are associated with our activities to determine appropriate and proportionate privacy and security safeguards or measures. We consider the state of our technology and user experience to determine what measures should be implemented.

Examples of safeguards includes:

- Following privacy by design and default principles
- Using only personal data in activities where it is necessary
- Undertaking risk assessments, audits, and reviews of our activities
- Aggregating, minimising, pseudonymising or anonymising data to reduce personal data
- Policies, procedures, and standards that govern the use of data
- Using privacy enhancing technology and using default privacy controls

- Having a detailed technical security framework which includes access limitation, encryption, and prevention against cyber attacks
- Having a Data Protection Officer to hold us to account for our activities

Changes to our activities

Our core activities do not change but where a new activity is identified or a change to this notice is needed, we will publish the changes and will make you aware only where the activity is not something you would reasonably expect.

4. 1st Central Connect.

If you purchase our 1st Central Connect telematics product, some of the information we collect and how we use it will differ from standard insurance because this product relies on driving and device data.

We are the controller for 1st Central Connect. Cambridge Mobile Telematics (CMT) acts as our processor for most processing, but may act as a controller for limited purposes where it determines how data is used, such as improving capabilities like crash detection. Information about CMT's use of data can be found in its privacy policy.

https://www.cmtelematics.com/privacy-policy/

We are not responsible for any processing of personal data that is undertaken by the provider of your personal mobile device. Please refer to their notices and your personal device manuals.

Product Suitability

When you decide to purchase a telematic based product you must agree to your driving being monitored. This includes your insurer being able to track you and your vehicle location when it detects that there is motion. We have implemented privacy defaults into our product to reduce any privacy intrusion, but we strongly recommend that if you are not comfortable with the use of location and tracking services that you consider the suitability of this product for you.

In addition to this notice we: -

Activity	Description	Reason
Send the Sensor to you and activate your mobile application (App)	We share your name and address with the supplier of the sensor device and your details with CMT. This ensures that a device is sent when a policy is purchased, and you can use the App. This will not include **sensitive personal data**.	Entering and Performance of the Contract.

Collection of data on the Mobile Application & Sensor	You must download our App on your personal device for the product to work. It is a condition of the Policy. The App along with the sensor is how we collect personal data.
	
	The technology is designed to capture:
	• how, when and where your car is driven,
	• device and sensor information at the time of capture:
	  • bluetooth
	  • location
	  • device ID
	• information related to your driving behaviours such as:
	  • speeding,
	  • phone use,
	  • hard braking,
	  • hard cornering,
	  • hard acceleration.
	
	The App and Sensor can independently and together collect personal data. We will only receive the data when the two are paired. You can see what is collected in the App directly.
	
	If technical issues are identified, we can force a call out to the application and sensor to help understand the problem and find a resolution.
	
	This will not include **sensitive personal data**.
		Entering and Performance of Contract
		
		There is a contractual obligation on you to ensure that when you drive the vehicle you have met the requirements of your insurance policy.
		
		Legitimate Interest in resolving technical issues for users.

Location Services	We use location services. The personal device will seek your location when it senses movement of the device, and this trigger the device to look for the sensor to pair with. As you use the vehicle it will then record location points. This provides us: • GPS Location • Distance travelled If the App cannot locate the sensor, then no recording is made, and nothing is stored or sent to us. The App will record that an attempt to pair the devices was made. We and CMT will not receive your location unless a recording is made. We receive associated information only. Your personal device will record the location attempt and will store the location information. IOS and Android devices store this information on your personal device which you can view at any time. They may present information to you as part of their location and privacy services. We do not control these notifications and do not see them. This will not include **sensitive personal data**.	Consent from subject to use the location services when the vehicle is in use.
Assessment of driving behaviours	CMT use artificial intelligence capabilities such as machine learning models to help them interpret and assess your driving skills and behaviours. This creates a scoring model that we use in our assessment of your driving behaviours, and which impacts your insurance price. You can see this data in your mobile application. An occurrence of a specific driving behaviour when scored for each trip is called an ***event***. For a trip, each event is assigned a risk assessment score. The overall score is a weighted combination of these. We use this information to inform our models for the insurance. It is this **personal data** that will impact our **automated decisions** on how to price your insurance. This will not include **sensitive personal data**.	Entering and Performance of Contract for assessment of the driving behaviours and scoring which impact the pricing of the insurance.
Interventions	We use this information to intervene if the data indicates that you need to make changes to your driving. The data we capture can also be used when an event occurs, such as an accident. We will use this data to: • intervene in the incident, • progress the claim, • or to act on your insurance if you're driving behaviour falls below our accepted threshold. We will use the mobile application and emails to notify you of the intervention and make recommendations for improvements. This will not include **sensitive personal data**.	Entering or Performance of the Contract

Claims Management	In the event of an accident, we use the data collected to assess the facts of the claim. It supports us in defending claims where you are not at fault. We can use the crash detection capabilities to support emergency services and you. Please note that collection of the data captured, and actions taken after are not an emergency service, and we are not an emergency service provider. This will not replace contacting the emergency services. This data may be shared with our legal panel, external supplier and other insurers in defence of claims. This will not include **sensitive personal data**.	Performance of the Contract
Device Tampering	We will use the data to identify and prevent misuse or tampering with the device. This will not include **sensitive personal data**.	Legitimate Interest
Product Enhancement	We will use the data collected to improve and enhance the product, user experience and technology capabilities and for statistical research. This will not include **sensitive personal data**.	Legitimate Interest

If you are not intending to drive the vehicle or use the cover, we recommend that you turn off location services on your device.

We cannot guarantee the accuracy of the technology or data, but we keep this under regular review and work to statistical accuracy thresholds. You have the right to challenge the accuracy of the data we use.

The mobile application design meets the standards that are set out by Apple (for Apple devices) or Google (for Android devices) for their application stores. There is notice information available in the App store and you can access the licence terms of the application in the 1st Central Connect App.

Data will start being collected the moment the sensor and application are paired for the first time. When you stop using the product it can take up to 72 hours for the data processing between you and CMT to cease.

We will retain your policy in line with our retention statement. We will also aggregate and anonymise data to support our statistical processing.

Who can see trip data in the App?

The technology can distinguish between you and other drivers through the mobile application device ID however there may be occasions when we cannot confirm who was driving. You will be able to see in your application how each driver is driving and how this impacts the driving scores**.**

It is important that you and all other product users understand:

- the sharing of this data in the application is the default setting
- we can make all trip data available to the policyholder as it impacts the insurance cover
- you can manage the accessibility of this information within the mobile application.

We will consider any external sharing of this data with law enforcement or other third parties on a case-by-case basis. We do not sell this data for commercial purposes. Please be aware that we may need to share information with CMT in the administration of the arrangement.

5. How will we share your information?

Sharing **personal data** is a necessary part of providing our services and protecting our customers. We will never sell your data, and we will only share it where we have a clear reason to do so. This may include sharing data where it is in our legitimate interests, and sharing arrangements are assessed through data protection impact assessments where appropriate.

If you need further information about a provider, we've detailed how to contact them in accordance with their notices and procedures.

5.1. Credit Reference Agencies

We'll perform credit and identity checks on you with a credit reference agency ("CRAs") such as Experian and TransUnion. When you take insurance services from us, we may also make periodic searches at the CRAs to manage your account. A record of those checks will be held by the CRA. On your credit file you'll be able to see those searches by a footprint labelled 'insurance search'.

We supply your **personal data** to CRAs, and they'll give us information about you. This will include information from your application and about your financial situation and financial history. CRAs will supply to us both public (including information on the electoral register) and privately shared credit, financial and fraud prevention information.

We'll use this information to:

- Assess whether you can afford to purchase the product
- Verify the accuracy of the data you have provided to us
- Validate the identity of subjects
- Prevent criminal activity, fraud, and money laundering
- Manage your account(s)
- Trace and recover debts
- Ensure any offers provided to you are appropriate to your circumstances

We'll continue to exchange information about you with CRAs while you have a relationship with us. We'll also inform the CRAs about your settled accounts.

We use CRAs to ensure the validity of the banking information we're provided. This service checks the details with the bank to ensure that the account is valid, will highlight data errors and will confirm that an account isn't linked to closed or fraudulent accounts.

If you're paying by direct debit, we may give details of your accounts and how you manage them to the CRA, including records of outstanding debt. This information may be supplied to other organisations to perform similar checks, to trace your whereabouts and recover debts that you owe. ***This footprint can be seen by others and may impact your credit score.***

If you tell us that you have a spouse or financial associate, we'll link your records together, so you should make sure you discuss this with them, and share with them this information, before lodging the application. CRAs will also link your records together and these links will remain on your and their files until you or your partner successfully file for a disassociation with the CRAs to break that link.

The identities of the CRA, their role also as fraud prevention agencies, the data they hold, the ways in which they use and share personal information, data retention periods and your data protection rights with the CRAs are explained in more detail at www.experian.co.uk/crain and Credit Reference Information Notice (CRAIN) | An Information & Insights Company (transunion.co.uk). We do not use marketing services provided by the CRAs.

To learn more about what information Experian holds about you or to request a copy of their full notice you can contact them at: Experian Limited, Consumer Help Services, PO BOX 8000, Nottingham, NG80 7WF www.experian.co.uk

To learn more about what information TransUnion holds about you or to request a copy of their full notice you can contact them at: TransUnion Information Group, One Park Lane, Leeds, West Yorkshire LS3 1EP www.transunion.co.uk

Insurance Industry Databases

We will pass and receive your **personal data** from the following insurance databases:

- Claims and Underwriting Exchange ("CUE")
- Motor Insurance Anti-Fraud and Theft Register ("MIAFTR")
- Motor Insurance Database ("MID")
- DVLA (MyLicense)
- DVSA (MOT)

We work in partnership with the Motor Insurers' Bureau (MIB) and associated not-for-profit companies who provide several services on behalf of the insurance industry. At every stage of your insurance journey, the MIB will be processing your personal information and more details about this can be found via their website: mib.org.uk.

Set out below are brief details of the sorts of activity we undertake:

- Maintaining databases of:
  - Insured vehicles
  - Vehicles which are stolen or not legally permitted on the road
  - Motor, personal injury and home claims
  - Employers' Liability Insurance Policies
- Managing insurance claims relating to untraced and uninsured drivers in the UK and abroad
- Working with law enforcement to prevent uninsured vehicles being used on the roads
- Prevent, detect and investigate fraud and other crimes, including, by carrying out fraud checks
- Supporting insurance claims processes

The data stored on these databases may be used by certain government organisations including the police, the DVLA, the DVLNI, the Insurance Fraud Bureau and other Insurance organisations allowed by law for the purposes of:

I. electronic licensing
II. continuous insurance enforcement
III. law enforcement (prevention, detection and catching or prosecuting offenders)
IV. providing government services or other services aimed at reducing the level and incidence of uninsured driving.

If you're involved in a road-traffic accident (either in the UK, the European Economic Area or certain other territories), the insurer, the Motor Insurer Bureau ("MIB") or someone making a claim (including their appointed representatives) may search the MID to get relevant information. It's vital that the MID holds your correct registration number. If it's incorrectly shown on the MID, you're at risk of having your vehicle seized by the police. You may check your correct registration number details are shown on the MID at www.askmid.com. Insurers have up to seven days to give the MID your details.

Requesting your data: Motor Insurance Bureau

We utilise the MyLicense service from the DVLA. If you choose to provide us your driver license number, we'll ask the DVLA to automatically provide details of your driving entitlements, the length of time you've held a driving licence, and valid motoring convictions. This information will be used in our insurance risk assessment of driving behaviour and premium and to prevent misrepresentation.

If you choose not to provide this, we ask you to self-declare the information instead. We'll repeat the call out and collection of this information when you're due for renewal to ensure we hold the most up to date information.

The information the DVLA provides us is subject to a set of standards and rules that we must comply with in addition to data protection legislation.

You can find out more about the information they hold at: DVLA privacy policy - GOV.UK.

We're responsible for ensuring the accuracy and security of the personal data we provide to these databases; however, we have no responsibility for the databases themselves, and information provided by other organisations.

5.2. Financial Transactions

To process financial transactions, we need to share financial information, such as payment details, bank account information and transaction details, with our payment providers and supporting technology providers. We use Adyen as our payment service provider to authorise, process and settle card payments, support fraud prevention, and help us manage refunds or payment queries. We may also use Bottomline to support payment processing and bank account validation, and Sycurio to support secure telephone payment capture and PCI compliance. If you'd like to know more about our providers:

Bottomline: https://www.bottomline.com/uk/privacy-policy
Adyen: https://www.adyen.com/policies-and-disclaimer/privacy-policy

Sycurio: PCI Compliance and Payment Security Solutions | Sycurio

Payment Standards
We're Payment Card Industry – Data Security Standard compliant. This means we have in place appropriate measures to manage and protect your payment card information. Our records contain the last 4 digits, the name on the card and the expiry date. When we need to use the card to make a payment, we ensure the gateway is encrypted to ensure data is protect in transit and at rest. We do not allow the transmission of this data, and our colleagues cannot access this data.

5.3. Fraud Prevention Databases

We're committed to ensuring we help to reduce fraud in the insurance market. Protecting our genuine customers and our business is critical and therefore we'll share data with law enforcement, government, banks, other insurers, and fraud databases where necessary to achieve this aim.

We complete our fraud activities in our legitimate interest for meeting regulatory requirements such as knowing our customer and anti-money laundering provisions as well as in our and your interests of detecting or preventing unlawful acts reducing insurance fraud more generally.

When we respond to a request for insurance or if there's a claim, or when you renew a policy, we'll repeat these activities to ensure our records remain up to date and we can make informed decisions.

Due to the nature of our purpose for processing we are unable to share detailed information with you about all our activities. This is so we don't prejudice any current or future investigations.

Identity validation and application fraud
It's important we know who we're providing services to therefore we can request you confirm your identity. In addition, if we have any suspicions that a policy has been misrepresented, we'll request that you provide documentation to check the accuracy of the record. Data inaccuracy can lead to additional premium and charges being payable.

Identity Fraud
We use technology to support us identifying individuals we suspect of being a victim of ID Fraud. We work with genuine customers or victims to ensure their insurance is valid or in accessing tools to protect their identity.

There's no one piece of information that tell us if someone has been the victim of fraud or is acting fraudulently, but we take a risk-based approach. This does mean that sometimes a genuine customer will be contacted. When this happens, we ensure the outcome is used to improve our approach.

Fraud prevention databases
The databases we utilise are joint **controllers** of the data. This is data that is collected from across the financial services industry. The **personal data** we share or receive can include your name, address, date of birth, contact details, financial information, employment details, vehicle details and device identifiers such as IP address.

It's important to understand that if you're considered to pose a fraud or money laundering risk or have been involved in fraudulent activity, the data they hold can be used by organisations to refuse services, financing or employment.

They work closely with law enforcement to prevent, detect, and investigate crime. They may transfer your **personal data** outside the European Economic Area for these purposes. In such cases this will be done in accordance with international transfer mechanisms and safeguards that the UK Government consider applicable.

We're unable to disclose what these databases hold about you, but you can contact them as follows:

Syndicated Intelligence for Risk Avoidance ("SIRA")
This is provided by Synectics Solutions. Synectics Solutions is a private fraud prevention agency which works with organisations in the fight against fraud and financial crime. Those organisations include businesses from the finance sector, insurance sector, communications sector and other sectors with a legitimate interest in preventing fraud, money laundering and verifying identity.
We may share personal data with SIRA and receive information from SIRA to help prevent, detect and investigate fraud, financial crime and misrepresentation. This may include information about your identity, contact details, policy, claim, payment, vehicle, device and transaction information. Synectics Solutions may use this information with data received from other organisations to identify fraud risks and support fraud prevention across participating sectors.
Where a fraud risk is identified, this may affect whether services are offered, continued or investigated. We can't disclose to you any information we receive from this database where doing so may prejudice fraud prevention, detection or investigation. If you'd like to know what information Synectics Solutions holds about you, you can contact them at:

SAR Department, Synectics Solutions Ltd, PO Box 3700, Stoke-on-Trent, ST6 9ET or DSAR@synetics-solutions.com
https://www.synectics-solutions.com/Portals/0/pdf/Subject%20Access%20Request%20Form%20V.3.3.pdf

Credit Industry Fraud Avoidance System ("CIFAS")
CIFAS is a not-for-profit fraud prevention membership organisation. They're the UK's leading fraud prevention service, managing the largest confirmed fraud database in the country. Their members are organisations from all sectors, sharing their data across those sectors to reduce instances of fraud and financial crime. They also assist us and our customers by offering protective registrations if they think they've become the victim of identity fraud. If you'd like to know what information they hold about you, you can contact them at:

CIFAS, 6th Floor, Lynton House, 7 - 12 Tavistock Square, London, WC1H 9LT www.cifas.org.uk
https://www.cifas.org.uk/contact-us/subject-access-request/subject-access-request-form

TransUnion ("Iovation")
Iovation is a provider of fraud prevention and account authentication services. Their services help us decide whether to accept transactions from electronic devices by analysing device attributes and checking whether they've been associated with fraudulent or abusive transactions in the past. The service also helps verify your identity by registering and remembering devices associated with your account. We'll share information with Iovation if we conclude that a device has been used in connection with a fraudulent or abusive transaction. Iovation track your activity over a network of different sites that subscribe to their services.

If you'd like to know more about how TransUnion process **personal data,** please see www.iovation.com/privacy. If you want to access the information they hold about you, you can contact them at: privacy@iovation.com.

Lexis Nexis
Lexis is a provider of modules that support our fraud and insurance activities. We use their modules to enrich our data and to validate no claims discounts and provide additional policy insights.

If you'd like to know more about how Lexis will process the data, please see Insurance Services | LexisNexis Risk Solutions. If you want to know access the information they hold about you, you can contact them at DPO@lexisnexisrisk.com.

5.4. Product Partners

To provide theProduct that's suitable for your needs we've formed relationships with a panel of trusted product partners. We'll provide your **personal data** to these product partners depending on what products you've bought, i.e. legal, excess, breakdown or personal accident.

You should check the policy wording for the products you have purchased to identify the details of the provider. The wordings contain the privacy notices of the provider who is the **controller** and will tell you how they process your information and how you can obtain access to the information they hold about you.

If you purchase the cover, we'll pass **personal data** for them to administrate their product, this includes your name, address, and contact information. This can include **sensitive personal data**.

Our product partners are all subject to contracts with us, and we require that they only use your **personal data** for the purposes of providing their services. We also place obligations on them to ensure a comparable level of security for your **personal data**. We monitor the products and services with our Partners to ensure they are fit for purpose and meet required standards.

5.5. Servicing your claim

The purpose of insurance is to ensure you can access services in the event you have an accident. To do this, we utilise a panel of repairers, engineers, recovery, and salvage services to help you along the way.

Our providers are all subject to contracts with us and we require that they only use your **personal data** for the purposes of providing their services and have a comparable level of security for your **personal data**. When we discuss the steps of your claim with you, we'll tell you which provider has been instructed to help you and why.

We instruct suppliers to:

- Provide vehicle recovery from the roadside or home
- Inspect and assess the damage to your vehicle
- Engage repairers to fix your vehicle
- Provide vehicle salvaging when a vehicle is damaged beyond repair
- Provision courtesy or hire cars
- Ensure ownership of the vehicle is managed
- Support us during the weekend and in the evenings
- Manage a claim following an accident in a foreign country
- Provide technology which allows the deployment and billing of repairs and recovery

When a vehicle is deemed a total loss as it's beyond economic repair the vehicle can be passed to salvage agents. We do perform reasonable checks to clear the vehicle of personal items and information. We provide you their details so that you can arrange collection of these. We can't guarantee that your personal information such as details from your motoring documents like the V5, service or logbooks etc won't be passed on to new owners of the vehicle. We don't expect them to contact you; however, this can occur if they require additional information or the spare keys.

Courtesy Car

We use Enterprise Rent-a-Car as our provider. We'll send over a referral to them containing your name and contact details to enable them to arrange the vehicle for you. Enterprise capture information for their own purposes and are a **controller** of that **personal data**. We recommend that you review their privacy policy which can be found at https://privacy.ehi.com/en-gb/home.html.

Image Capture and Engineering Services

First Central Insurance Services (ReCentra) will jointly and independently with the Controllers collect and store data to perform the engineering assessment of your vehicle. This will include requesting images of your vehicle.

Others

We may need to instruct other providers to help us such as specialist engineers or repairers on a case by case basis. If this needs to happen we'll let you know.

Legal Panel

Another part of the insurance services we provide to you is to put you in contact with Solicitors who can help you with any legal claims you may have. We also instruct Solicitors to help us defend claims where we're being pursued by other insurance companies following an accident.

Our legal panel is made up of several firms, each providing expertise in an area of law or in certain jurisdictions. Each member of our legal panel is regulated by the Solicitors Regulation Authority and has the same obligations we do under the data protection law.

Personal data will only be shared with our legal panel for the purposes of pursuing or defending legal claims. We'll let you know which firm is instructed. When they contact you, they'll expressly confirm we have instructed them. If you accept their services, they'll become a **controller** of your **personal data**.

They'll have their own privacy notice which they'll make available to you. If you receive telephone calls from any other law firm who we haven't advised you about, please let us know.

5.6. Reinsurance Panel

As an Insurer, we need to have insurance to cover the insurance we provide you. We do this through a reinsurance panel. The panel consists of many companies. You'll never be directly contacted by members of the reinsurance panel. The panel are Data Controllers.

We've introduced privacy by default into our arrangements with the panel. This means that they'll never be provided your **personal data** unless there is a specific legal or regulatory reason to do so. If **personal data** does need to be passed to a panel member, the data will be minimised to what's necessary.

5.7. Debt Recovery

If you pay by direct debits and you fail to make payments, we'll appoint a debt-recovery agent to support us in collecting any outstanding balance. We understand you may not want us to share your information for this purpose; however, we consider this this to be in our legitimate interest for recovery of the money payable under your insurance contract. Debt recovery services will be provided information from credit referencing agencies. We may sell our debt to the debt recovery service providers. If we do this, you will be written to. Once this data transfer has occurred the debt recovery service provider will become the Controller of the processing.

We'll only share **sensitive personal data** if you consider yourself a vulnerable customer to enable our colleagues to ensure you're treated appropriately.

5.8. Group Companies

Personal data may be shared between the companies in the First Central Group for the purposes of providing its services and business administration. You can find out more about the companies in our Group by visiting: www.firstcentralgroup.com.

5.9. Outsource Partners

We use companies to provide services as outsourcers, for example, we have a contact centre which is provided to us by an outsource partner. If a supplier is an outsourcer, they'll present themselves as 1st Central.

We'll remain the **controller** of your **personal data** and they'll act as a **processor** on our behalf. Our outsource partners are all subject to contracts with us and we require that they only use your **personal data** for the purposes of providing the service and on our written instructions. We require them to ensure a comparable level of security for your **personal data**.

As they are **processors,** we have additional responsibilities to ensure that they're **processing** the **personal data** in accordance with the law, and we conduct regular due diligence and monitoring.

6. How will we communicate with you?

Types of Communications

Service

As an online company, we prefer to communicate by email, however there may be occasions where we use SMS, telephone, or post. It's important we have up to date information for this purpose. These communications will be about your policy or claim. We'll communicate with you if we need you to act, to send payment reminders or to remind you about your renewal. Communications will be available in your portal. You cannot opt out of service communications as we consider these essential for you to see and us performing our contract with you.

Survey and Feedback

We provide opportunities for you to provide feedback on our services. Our surveying is used to help us to improve the process or product we are offering. You do not need to participate in these surveys. Surveys can be emailed or appear in online portal if you use our online services. If you do not wish to receive surveys by email, contact us.

Marketing

Our marketing communications are only sent to customers who have consented to receive these. All our marketing contains a link that allows you to unsubscribe at any time and you can manage your preferences in your portal. Marketing promotes new products or promotions, offers rewards or competitions.

Modes of Communication

Telephone Calls

We make and receive telephone calls through our contact centre. We do record a sample of our telephone calls and a notice of this is given at the outset of a telephone call in our messaging. If we contact you by telephone and there's no response, we can leave a voicemail, but we don't do this every time. We do have services available for accessibility purposes. We do transcribe call recordings for use in analysis activity to help us improve how colleague communicate with you.

Web-Based or Telephone Chat

We provide chat functionality on our website. This includes webchat, social channels and WhatsApp messaging capabilities. We use chatbots to support with locating information on our website and helping to complete online actions. We may also use telephone-based conversational automation, including audio-based bots, to support simple manual tasks such as routine policy servicing and policy cancellations. We also have colleagues available where your questions or requests cannot be supported by our automated tools.

7. Cookies

There are two types of cookies we use, those that are *strictly necessary* or those that are for *tracking or targeting.* Strictly necessary cookies are those we need to make the website function, keep it secure and detect malicious activity. These cookies also give us functionality to remember you within any visit to our site. They help us tie together your web experience together as you move from page to page, remembering your inputs from the previous page. Strictly necessary cookies will automatically be enabled. You can manage your preferences on our website.

These can include: -

- *Accelerated Mobile Pages ("AMP")* - AMP allow for pages to load more quickly on a mobile device by allocating a Client ID to that device where the web page had been loaded before.
- *Iovation* – we use these cookies to prevent and detect devices associated with fraudulent or other malicious activity. JavaScript collects information about the attributes of your device, such as IP addresses, device type, browser type, screen resolution and operating system. This information is shared with Iovation Inc, for fraud prevention and account authentication purposes. For more information about Iovation, please see www. iovation.com.
- *Genesys* - These cookies are used in our web chat service; it enables our handlers to see which pages you interacted with to better support your questions when using this service.

Tracking and Targeting cookies are those that provide further functionality to our website but will also enable us to monitor how our website is interreacted with and personalise the journey. These cookies can be session or persistent meaning they'll either expire when you leave the site or remain active for you to return to the site and recall any information you entered.

You can also choose to disable tracking and performance cookies in your browser. See our Cookies notice for more information.

8. Security

Our customers are at the heart of the services we provide; therefore, the security of your personal data is very important to us. We've put in place organisational and technical measures to protect your information from unauthorised access, use and loss. We safeguard your privacy and will continually monitor our measures, updating our approach as new technology and industry best practice becomes available.

Site security

We ask you to set a unique and strong password to help us protect your information in the portal. This password is used to access your policy information and documents online. If you've forgotten your password or email address, you can retrieve them on the Account Recovery page.

To protect your information, we use the industry standard Secure Sockets Layer ("SSL") 128-bit encryption technology to ensure that all your personal and transactional information is encrypted before transmission. Depending on your browser you should see a closed lock or unbroken key in the bottom left-hand corner or in the URL bar to signify that SSL is active and you're in a secure area of our site.

We aren't responsible for the privacy policies and practices of other websites, even if you access them using links from our website and we recommend that you check the privacy policy of each site you visit.

Information Security Management

We are ISO270001 Information Security and Payment Card Industry Standard accredited. These external accreditations help demonstrate that we have in place adequate and appropriate security controls to protect the **personal data** we collect, process and store. We also operate a cyber security framework in accordance with industry practice to reduce the risk of cyber-attack.

9. International Transfers

The information we hold about you is encrypted during transfer and at rest. It's stored securely in private dedicated server environments within the UK and EEA. Some information may be stored on servers outside of the UK and EEA. If your information does need to be transferred or stored outside of the UK or EEA for us to perform our activities, we'll ensure that this is done securely and in compliance with the law.

We have put in place a standard which sets out our approved countries for transfer. These countries must have in place adequate frameworks and legal protections for our customers. We will use mechanisms such as the approved standard contract clauses or international data transfer agreements recommended by the authorities when performing these transfers. Countries include but are not limited to: Guernsey, Gibraltar, South Africa and Ireland. If you would like to know more about international transfers, contact DPO@1st-central.com.

10. Artificial Intelligence

We do use Artificial Intelligence (AI) capabilities whether integrated into the technologies we use or as standalone technology. We use the capabilities to aid in our daily operations to benefit you and our colleagues. All usage of these technologies is subject to assessment and oversight by our Data Protection Officer.

We may use AI-assisted technologies when you interact with us through certain customer service channels. These technologies may process information you provide during conversations, together with policy and account information, to understand your enquiry, support policy administration, improve customer service and monitor service quality.

We are committed to: -

- offering explainability and transparency where the capability makes any decision about you.
- ensuring fairness, non-discriminatory ethical use through human oversight.
- using secure, safe, and robust capabilities that meeting legal and industry standards.
- having governance and accountability for our usage at senior levels.
- offering redress and contestability for any wrongdoing.

AI forms part of our long-term plans. As our use of AI expands, we will continue to provide layered information within your experience with us. We will minimise the personal data used and will only use AI where we can secure the environment and maintain appropriate control over the processing.

11. Wholly Automated Decision Making

To provide our services we make wholly automated decisions that will involve profiling. We evaluate certain personal aspects about you such as your economic situation, personal preferences, driving behaviour to make these decisions. We make these decisions as it's necessary to entering and performing the contract, to meet regulatory obligations and prevent and detect unlawful acts.

We do this to:

a) Determine insurance risk
b) Determine affordability
c) Detect and prevent unlawful acts – fraud

Where we conduct these activities, we're required to inform you of the type of information we collect or use in creating the profile or making the decision, why this information is relevant, what the likely impact is going to be/how it's likely to affect you.

Please be aware that this doesn't mean we're required to disclose our actual algorithms or intellectual property such as how the assessment prices our products but can provide meaningful logic to help you understand the decision-making process.

a) Determining insurance risk

The assessment for providing motor insurance is a determination and scoring of factors in two categories. Firstly, factors about an individual or individuals proposed to be driving the vehicle and secondly factors about the vehicle itself. Each insurance company has defined what risk profile they can insure and what factors they are looking for. This allows for us to provide products that can meet the needs of the customer. You provide us these factors when you obtain a quote from the price comparison website. This is a necessary assessment for entering the insurance contract.

The factors we collect and use to create a driver and vehicle assessment include:

- The date you and additional drivers passed their driver's test
- Yours and any additional drivers - driving history
- Yours and any additional drivers - claims history
- Occupation and use of the vehicle
- The type of vehicle being covered
- Modifications and safety
- The age of the vehicle
- The value of the vehicle
- The location of the vehicle during the day
- Storage of the vehicle overnight

For example, we ask you how long you have been driving, or how many accidents you've had in the last 5 years, from this we can draw inferences as to your driving experience. The less experience you have may mean you're a higher insurance risk. We'll ask you the price of the vehicle, where it'll be parked and how it'll be used as this can help us to consider security of the vehicle and the levels of cover needed to protect the use of it.

Different makes and models of cars can vary in features or have modifications. If an older vehicle is damaged it can be harder to source the parts, newer vehicles may have more sophisticated technology requirements.

All the factors are scored and from this we can determine the cover level, the product, and our pricing. If the scoring profile goes outside our threshold, then a consequence maybe that we can't offer you cover as we don't have a product to meet your needs. This doesn't mean that you won't be covered with another company, simply that we've determined the risk isn't suitable for us.

We only consider information relevant to the decision-making process for providing motor insurance. We don't ask for information that's unnecessary. For example, we don't need to know about accidents you had 20 years ago as this wouldn't help us understand your most recent driving experience.

If you are a 1st Central Connect customer your driving data will additionally be used in the insurance risk decision.

We will also use publicly available and industry-accessible data about claims and vehicles to support models that help us determine risk.

b) Determining affordability

We're a consumer credit provider. This allows us to offer the ability to pay for insurance in monthly instalments. We're required by regulation to conduct affordability assessments for every applicant to offer this financial product.

We do this at the same time as determining the insurance risk to provide you a complete quote with payment options and repeat this assessment when changes happen midterm and at renewal. For this assessment we use personal data we receive from credit referencing agencies, specifically the credit score, judgements, and any defaults, along with your payment history to determine whether our financial product is suitable for you and your creditworthiness. If you have several defaulted accounts, we may not consider it responsible to accept a credit application therefore we'll offer a pay in full option only.

c) Detecting and preventing unlawful acts – Fraud

We do this at the same time as determining the insurance risk. Decisions at this point will be made using external sources of data. For details of those external sources please refer to the how we share your data – Fraud Prevention section of this notice. The decision made will also take into consider publicly available information issued by the government and by fraud prevention enforcement services. Our primary purpose is to ensure the accuracy of the data we have and to ensure we have the identity of customers.

We are unable to provide information about the rules and logic we apply to the detection and prevention of unlawful acts as to do so would prejudice the purpose of the activity.

Safeguarding our wholly automated decisions

We use recognised actuarial models that prevent errors, bias, and discrimination. We regularly analyse and monitor these models to check the quality of the decisions being made. This is closely monitored against the wider insurance market.

We recognise that inaccuracies of data can occur therefore we've put in place safeguards and processes to review the decision and to correct inaccurate data if identified. It important that you provide us an accurate representation of your needs. As these are wholly automated decisions you have the right to request human intervention. We'll consider your point of view or challenge to the decision, however a right to request a review doesn't mean we're required to change our decision.

Third Parties

We use information obtained from third parties in these processes. They each provide certain data sets that validate, enrich, and support the data you've provided. The third parties are documented in this notice. Each of these third parties are Data Controllers. We aren't responsible for the accuracy of the data they hold and provide us. If you'd like to know what they hold about you can find out more by contacting them.

12. How long will we keep your information?

We will only keep information that identifies you for as long as it is needed to perform our activities, meet legal and regulatory obligations, defend or pursue legal claims, support our legitimate interests, or manage fraud-related concerns.

The **processing** we undertake in our legitimate interest for development of our services and products uses minimised data and where possible uses anonymous information as standard.

Examples of our legal obligations: -

- The financial conduct authority requires 5 years of record keeping minimally
- Anti money laundering regulations requires 5 years of record keeping minimally
- Reinsurance requirements extend up to 15 years
- Credit referencing is 6 years minimally
- MID, CUE and MIAFTR is 7 years minimally
- Court Limitations range from 6 – 15 years depending on the jurisdiction

Our longest retention for Motor is 25 years but there is information that could be retained indefinitely. This is very limited but would relate to lifelong claims, specific legal obligations, law enforcement or fraud activities.

Our cleansing approach takes place over time meaning as data ages we weed our records. We factor in the systems, usage and time to ensure that as we approach the longer retentions, we hold the bare minimum needed.

13. Your Rights

The law gives you rights over your personal data, although not all rights are absolute. We review each request based on the circumstances and will do our best to help where we can. When we receive a request, we may need to confirm your identity and clarify what you are asking for. We normally have 30 days to respond, but this can be extended where a request is complex.

You can exercise these rights directly with our Data Protection Officer by email at DPO@1stcentral.co.uk or in writing to our registered address.

13.1. The right of information

This right enables you to be informed about the collection and use of your **personal data**. We take a layered approach to providing this information. You were directed to review our basic privacy notice when you were purchasing your cover, and we provided a shorter version in your policy wording. This document is our full notice.

13.2. The right of access

This is more commonly known as submitting a ‘data subject access request’. We recommend you make the request in writing. This right enables you to obtain confirmation that your **personal data** is being processed, to obtain access to it, and to obtain other supplementary information about how it’s processed. We recommend that you review your customer portal, as much of the information we hold is available there.

We’ll conduct reasonable and proportionate searches for information. There may be information that we can’t disclose. If this is the case, we’ll explain our decision and the lawful exemption we’re relying on.

We can refuse to accept requests if they are unfounded or excessive. The right of access is not the same thing as asking for copies of a file. We are only obligated to provide the personal data and description of processing.

13.3. The right of rectification

If you see that any of the **personal data,** we hold about you is inaccurate, you can ask us to update it by contacting our Customer Services team. You can also update information directly in your customer portal at any time.

13.4. The right of erasure

You have a right to be forgotten, but this will only apply in certain circumstances. If these circumstances aren’t present, we’ll take steps to record your request and ensure that at the correct time your information is erased, we’ll cease any marketing. We’ll also suppress your **personal data** in order that no further **processing** can occur using your information. Our Customer Services team can help you to remove payment cards and close your accounts.

*13.5. The right to object to **processing***

You have the right to tell us to stop marketing to you and you can object to **processing** activities where we don't have a legitimate interest to conduct the activity. We've made it so you can manage your marketing preferences at any time in your customer portal without needing to contact us.

*13.6. The right to restrict **processing***

You have the right to request restriction or suppression of your **personal data**. This isn't an absolute right and only applies in certain circumstance. For when to exercise this right, please visit the website of the Information Commissioner. We'll respond to any requests within 30 days.

13.7. The right of data portability

You can obtain a reusable copy of the information you provided us within your customer portal; this can then be used for your own purposes. We aim to provide the portable data within five days of your request, but we do have 30 days.

13.8. Rights relating to automated decision making

You have a right to request, that an automated decision with profiling which has a significant or legal effect, is reviewed. The most common reason you may make this request is if you believe the data, we've used is inaccurate. You can do this by contacting our Customer Service team who will investigate this matter for you.

14. Concerns

If you're unhappy with how we've handled your personal data, you can raise a complaint. All complaints will be acknowledged and responded to within 8 weeks. You can contact our Data Protection Officer by email at DPO@1st-central.com or in writing to, Capital House, 1-5 Perrymount Rd, Haywards Heath, RH16 3SY.

Following this, if you remain dissatisfied, you can escalate your concerns to the Information Commissioner's Office as the UK's independent body empowered to investigate information handling practices. You can visit www.ico.org.uk for more information about this.

15. Definitions

These are the key terms used in this notice with their legal definitions:

Controller	The natural or legal person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of the processing of personal data.	**Personal Data**	Any information relating to an identifiable natural person. They can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
Processor	The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. They do not determine their own processing activities.	**Special Categories of Personal Data**	This includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data or data concerning an individual's sex life or sexual orientation, and the processing of genetic data or biometric data for uniquely identifying an individual.
Subject	The legal person that the personal data is about, for these purposes this is "You".	**Conviction Data**	The data relating to any motoring related convictions that the subject has disclosed on their insurance application.

Legal Basis	The legal basis which the Controller relies on to undertake its processing of personal data as guided by the law Including: ▪ Legitimate Interest ▪ Consent ▪ Entering into & Performing a Contract ▪ Insurance ▪ Legal Obligation ▪ Public interest ▪ Vital interest
Processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means or not, 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.