Using my personal data

Full Privacy Notice

Introduction

Thank you for choosing a 1ST CENTRAL product. When you applied for, interacted with our website, or purchased insurance with us, you were asked to review our online privacy notice which provided summary information about our use of your personal data. This notice provides additional information, that as a valued customer, you should have to understand how we'll 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 purchase the 1ST CENTRAL Insurance product:

First Central Insurance Management

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.

Skyfire Insurance Company Limited

They're the insurance provider and underwrite the 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 Crutchetts Ramp, Gibraltar GX11 1AA

Contact the **Data Protection Officer** at DPO@1stcentral.co.uk.

The **controllers** will together or separately determine the **personal data** collected, the **lawful reasons** for **processing,** how that **personal data** may be shared and for how long we'll store the **personal data**.

2. What information do we collect?

We'll collect the following **personal data** directly from you during your application for insurance:

Personal information

- Your full name and title
- Full address and postcode
- Date of birth
- Marital status
- Gender
- Employment status and position
- Telephone number
- Email address
- License number
- Vehicle registration, make and model, modifications
- Claims history
- Residency
- Home ownership
- Accident location
- No Claims Discount

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 – From website

- IP address
- Device ID

Information you give to us on behalf of others

- Named driver – full name, date of birth, employment status, license numbers and **conviction** information
- Third party payers – the payment information 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

We'll also collect data from third parties, law enforcement and insurance industry databases including:

- Credit score, default Information, county court judgements/IVAs and financial history
- Identity fraud markers
- No Claims Discount
- Driving entitlements
- Device Information
- Vehicle MOT and Tax history

3. How will we use your information?

If you're a prospective customer or customer of ours, we'll use **personal data** to perform certain activities. We don't do anything you wouldn't reasonably expect or perform activities with unjustified effects. We've detailed our **lawful basis** for those activities using **personal data** and our secondary basis for using **sensitive personal data**. If we perform an activity that's in our legitimate interest, we've detailed that interest and we'll ensure that we balance this against your rights to privacy.

Activity	Description	Reason for Activity
Providing you a quote for insurance	Whether you come directly to us or through a price comparison website, we'll process the **personal data** you've provided to evaluate the insurance risk and provide a quote for insurance. We undertake this activity through **modelling** and the decision is made by **solely automated means** that include **profiling**. See section 8 for more information. This includes **sensitive personal data** such as conviction and health data.	Necessary for entering and performance of a Contract. Substantial Public Interest – Insurance Purposes
Providing you a quote for finance	We'll assess your ability to pay for our insurance product through an affordability assessment. Our assessment follows regulatory guidance and requirements. This decision will determine if we can offer you finance for our product and on what terms. We undertake this activity through **modelling** and the decision is made by **solely automated means** that include **profiling**. See section 8 for more information. This doesn't include **sensitive personal data**.	Necessary for entering and performance of a Contract.
Accepting payment of deposit and future payments	If you purchase a product, we'll need to process **personal data** to collect the deposit, full payment or set up direct debits. *Paying Online*: Our website is designed securely to capture the payment information and to send it directly to the payment gateway for your banking provider. *Pay by Telephone*: You'll enter the details on the telephone keypad, and this will automatically transfer to the payment gateway. The details won't be captured in our calls or seen by our employees. *Direct Debits*: If you want to pay by direct debits, we'll capture your bank instructions. We use a banking service to ensure the accuracy of the bank account information we're given. The payment card will be retained for the duration of your policy to ensure we can support you in future transactions, at renewal, fraud purposes and if any refunds become payable. We use Continuous Card Authority (CCA). Please refer to our policy wording and credit agreement for more information about CCA and your rights. You can withdraw CCA at any time. This doesn't include **sensitive personal data**.	Necessary for entering and performance of a Contract. Substantial Public Interest – Insurance Purposes Legal Obligation – refunds must be paid to the original payment card to prevent money laundering.

Providing your insurance cover and services	We need to undertake activities for the administration of your insurance contract with us including: ▪ Setting up your policy ▪ Validation of your identity ▪ Cancellation and automatic renewal of your policy ▪ Providing customer care through email, social media, live chat, and telephone ▪ Handling any issues or complaints ▪ Providing access to your ancillary products and to other policy benefits including managing vulnerable customers Discrepancies in data could lead to your insurance policy becoming invalid, therefore it's necessary we have an accurate record. We'll contact you to discuss inaccurate data and ask you to provide documentation for validation purposes. This includes **sensitive personal data** where you request support as a vulnerable customer.	Necessary for entering and performance of a Contract. Substantial Public Interest – Insurance Purposes
Providing ancillary products	If you purchase an ancillary product: Breakdown Cover, Hire Car Cover, Legal Expenses, Personal Accident Cover or Excess Protection, we'll process your **personal data** with the insurer and intermediaries for those products at sale to enable them to provide their services. See section 4.5. They're **controllers** for this purpose. We recommend you consider their privacy notices which are available in the applicable policy wording for the product on our website. This will include **sensitive personal data** if you've purchased Personal Accident Cover.	Necessary for entering and performance of a Contract. Substantial Public Interest – Insurance Purposes
Updating Industry Databases	We're required to notify the Motor Insurance Database (MID) when an individual purchases insurance, the Claims Underwriting Exchange (CUE) or Motor Insurance Anti-Fraud and Theft Register (MIAFTR) of any claim activity. This will include **sensitive personal data** where personal injury is involved.	Legal Obligations – under the Road Traffic Act and Insurance Directives
Claim handling	If you're involved in an accident, we need to undertake activities to provide you services: ▪ Setting up the claim ▪ Deploying providers to collect, assess, value, or repair your vehicle ▪ Providing access to your ancillary covers ▪ 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 ▪ Handling reinsurance ▪ Recovering any money This can include **sensitive personal data** where personal injury is involved.	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 Recovery	If we need to recover any money from you in respect of missed payments under your finance agreement, we'll pass your **personal data** to a debt recovery agent for this purpose. This activity includes: ▪ contacting you to discuss payment arrangements ▪ setting up payment plans ▪ sharing information with credit referencing agencies ▪ progressing legal action If we need to recover any money from you in respect of a claim, our claims team will discuss this with you. We'll conduct legal recovery where necessary. This can include **sensitive personal data** where you request support as a vulnerable customer.	Legitimate Interest – recovery of monies payable under the insurance contract. If you'd like us to record a vulnerability, we'll flag the record, any additional information we'll record with your permission.
Fraud Analysis, Investigation, and Intelligence	We're committed to reducing insurance fraud to the benefit of our customers and the wider insurance market. We perform analysis, investigation, and intelligence activities to do this. We consider these activities to be sensitive in nature and have dedicated teams with specialised training to conduct them. We've implemented measures and safeguards as detailed in this notice to protect your privacy and ensure no unjustified impact occurs when conducting these activities. We balance our purpose with your rights; however, it isn't always appropriate for us to provide additional information where to do so could prejudice the purpose of the activity. We can confirm: ▪ We'll collect and use public sources of data such as government advisories, the national crime agencies, national fraud databases, social media platforms when conducting these activities ▪ We'll use private sources of information 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'll use investigation services to support in our activities ▪ We do use personal and sensitive personal data to profile individuals and in other forms of automated processing during these activities ▪ We'll share our findings with appropriate authorities and law enforcement ▪ We'll retain fraud information if it's relevant and necessary This can include **sensitive personal data.**	Legitimate Interest – protection of you and us and to meet regulatory requirements Substantial Public Interest – prevention and detection of unlawful acts Substantial Public Interest – Insurance Purposes 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 telephone calls ▪ monitoring customer service ▪ considering any feedback from you ▪ considering any industry benchmarking ▪ the suitability of our products and partners ▪ using speech-based technology ▪ monitoring any complaints and rootcauses We'll send you feedback surveys at the end of a new transaction or a claim. They're not mandatory but provide an opportunity to feedback about your experience. We record a sample of our telephone calls. These can include **sensitive personal data**. The other activities don't include **sensitive personal data.**	Legitimate Interest – product and service monitoring Substantial Public Interest – Insurance Purposes
Service Communication	We'll contact you regarding your insurance and our services. This will include updating you about our insurance documentation, your policy, your claim, and your finance. This can include our opening hours, updated insurance documents, renewal invite reminders, payment reminders, updated contact details. All these communications will also be available in your customer portal. We'll send service communications by email and SMS. These communications don't include promotional or marketing materials. This doesn't include **sensitive personal data.**	Legitimate Interest – keeping in contact with you about your insurance
Marketing	We want to keep in contact and send you details of our offers and products. We do this by email, telephone, SMS, and post. You can opt out of this at any time. 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. Every communication has a clear and easy unsubscribe option. We also have a preference centre in your customer portal to ensure you have control over the marketing you receive, and you can access this at any time. We do conduct marketing campaigns with partners, but we don't, under any circumstance, sell our marketing records to third parties. This doesn't 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 our offers and rewards to your needs ▪ remembering you on our website and welcoming you back This doesn't include **sensitive personal data**	Legitimate Interest – customer journey and experience
Business Administration	As a company we're subject to business administration activities to ensure we can comply with regulatory or legal obligations. These 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 finance and accounting ▪ manage issues ▪ make decisions about our products and services ▪ manage manual processes This doesn't include **sensitive personal data.**	Legitimate Interest – management of a business
Legal or regulatory Requirements	We may have to process your **personal data** to meet our legal obligations. In most cases we can use anonymised information but on occasion we do have to provide **personal data**. This includes complying with: ▪ court orders for disclosure ▪ financial reporting ▪ 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 do support and use technologies which have artificial intelligence capabilities. This includes robotics and machine learning. The tools are used to support activities recorded in this notice. We have a framework for management and safeguarding the use of these technologies. Please see our Cookie Notice for information on the use of Cookies on our website. This can include **sensitive personal data**.	Depends on the activity it's supporting.

Product Development and Innovation	We use personal data we've collected to help us improve or create new products. 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 do not make any solely automated decisions with profiling about individuals as part of our development activities. If the activity leads to this when implemented the details of those activities are recorded in this notice. These activities can include: ▪ Statistical analysis on our pricing and risk models ▪ Product governance monitoring ▪ Improving our website and customer portal journeys and functionality ▪ Improving our product documentation ▪ Understanding issues and rootcauses ▪ Benchmarking against the wider industry ▪ Obtaining data from third parties to enrich our models This could include **sensitive personal data.** In such cases it will be pseudonymised, aggerated or anonymised to create new data sets.	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

What If I'm not a prospective customer or customer?

I was a witness to an accident with your customer how will you use my personal data?	We'll collect your **personal data:** ▪ To help us investigate the claim ▪ To detect and prevent fraudulent claims ▪ Communicate with you about the claim We might need to share your information with other insurers, legal representatives as part of this process. We'll retain your information as part of managing the claim. This could include **sensitive personal data** depending on what you advise us.	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 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 will be 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

Sensitive Personal Data and Conviction Data

We ask you to provide information which the law classifies as **sensitive personal data**. This is limited to health, and personal injury in a claim or information you provide about vulnerability to ensure you receive appropriate treatment. We can infer **sensitive personal data** specifically your ethnicity from residency and identity documents.

We'll also ask you to provide information relating to **criminal convictions** or alleged or actual criminal offences, specifically related to motoring as this does play role in assessing driving behaviour.

Where we collect **sensitive personal data** or **criminal conviction data**, we process this data because it's in the substantial public interest to do so for the purposes of arranging and/or advising on contracts of insurance, claim handling and prevention and detection of unlawful acts relating to Fraud.

We have a policy and standard for use of **sensitive personal data** or **criminal conviction data** for ensuring we safeguard your privacy. This information can be shared in limited circumstances as it relates to the purposes identified.

Children

We aren't a direct provider of services to children; however, we'll have to capture information relating to a child if they're involved in an accident and we're required to offer claim services. 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.

Safeguarding our Activities

We consider the data protection principles and risks that are associated with our processing 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 measures and safeguards includes:

- Following privacy by design and default principles
- Ensuring privacy control defaults
- Undertaking risk assessments, audits, and reviews of our activities
- Aggregating, pseudonymising or anonymising data
- Policies, procedures, and standards that govern the use of data
- Having a Data Protection Officer to hold us to account for our activities
- Using privacy enhancing technology
- Having a detailed technical security framework which includes access limitation, encryption, firewalls

4. How will we share your information?

The sharing of **personal data** is a necessary part of us being able to provide services and protect our customers.

We make a commitment to you that we'll never sell your data or share your information without a clear reason to do so. If that sharing of information isn't what you'd reasonably expect, we'll let you know.

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

4.1. Credit Reference Agencies

We'll perform credit and identity checks on you with a credit reference agency ("CRAs") namely Experian. 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'. ***This footprint can only be seen by you and us and won't affect your credit score.***

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
- 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.

We don't use any 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

4.2. Insurance Industry Databases

We have legal obligations that require us to pass your **personal data** to the following insurance databases:

- Claims and Underwriting Exchange (CUE)
- Motor Insurance Anti-Fraud and Theft Register (MIAFTR)
- Motor Insurance Database (MID)

These obligations are imposed under legislation such as the Road Traffic Act. All the databases are operated by the Motor Insurance Bureau. Every insurer must be a member and follow membership rules to maintain their access to these databases.

The **personal data** passed to these databases will include your name, date of birth, vehicle registration, policy number and the date of any accident and related circumstances. This information is passed in a secure, encrypted feed to ensure they're regularly kept up to date.

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.

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. If you'd like to know what information these databases hold about you, you can contact them by completing a subject access form available at: **https://www.mib.org.uk/managing-insurance-data/mib-managed-services/cue-miaftr/**

Please indicate in your request which database you are enquiring about and what information you require.

4.3. Finance Transactions

To process financial transactions, we need to share financial information such as your payment or bank account information and transaction details to our payment providers and supporting technology providers. If you'd like to know more about them:

Bottomline: https://www.bottomline.com/uk/privacy-policy
Verifone: https://www.verifone.com/en/us/legal

Payment Standards
We're Payment Card Industry – Data Security Standard compliant. This is externally assessed. 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 our payment gateway is encrypted at every stage.

We use Semafone as our provider to ensure we comply with these standards. If you would like to know more about them: https://semafone.com/gb/privacy/.

4.4. DVLA/DVLA(NI) & MIB

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. The information won't be accessible by our Colleagues and isn't printed on policy documents.

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 www.mylicence.org.uk.

4.5. Fraud Prevention Databases

We're committed to ensuring the 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 can't share detailed information with you. This is because we don't want prejudice any current or future investigations. Each case is considered on its merits and we'll provide transparency where possible.

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.

We provide access to a secure portal that the documents can be uploaded to. These will be reviewed, and we'll let you know if there's any further action needed. The documents will be retained as part of the insurance 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. In these cases, we'll contact the individual. We can then work with genuine customers or victims to ensure their insurance is valid or in accessing tools to manage their identity. There's no one piece of information that tell us if someone has been the victim of fraud, but we take a risk-based approach. This does mean that sometimes a genuine customer will be contact. 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, therefore you'll need to contact them directly. You can do this 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. Those organisations include businesses from the finance sector, insurance sector and communications sector. We can't disclose to you any information we receive from this database. If you'd like to know what information they hold 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 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 that help us to validate your no claims discounts or to provide policy insights.

If you'd like to know more about how Lexis will process the data please see www.risk.lexisnexis.co.uk/consumer-and-data-access-policies/insurance. If you want to know access the information they hold about you, you can contact them at DPO@lexisnexisrisk.com.

4.6. Product Partners

To provide the 1ST CENTRAL Product 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 brought.

1ST Rewards
If you purchased a policy prior to June 2020 you'd have been referred to 1ST Rewards for additional benefits as part of you cover. The rewards portal was powered by Sodexo Motivation Solutions and enabled you to have access to discounts and benefits from unconnected third parties. We provided them the policy number, name and email address and they contacted you to create an account. This was an optional benefit. If an account was created, you were asked to agree their privacy policy and they became the **controller** of the **personal data**. If you'd like to know more information about how Sodexo process data please see https://www.sodexo.com/home/legal--privacy/global-data-protection-policy.html.

Legal Expenses, Personal Accident, Hire Car, Breakdown, Excess Protect – Ancillary Products
You should check your ancillary policy wording to identify the details of the insurance provider. This contains the privacy notice of the **controller**. If you purchase the cover, we'll pass **personal data** for them to administrate their product, this includes your name, address, contact and vehicle details. This may include **sensitive personal data** for vulnerable customers.

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 place obligations on them to ensure a comparable level of security for your **personal data**.

We recommend that you familiarise yourself with their privacy terms for more information on what they may do. The contact details for each of these providers is available within the applicable policy wording.

4.7. Claims Repair and Recovery

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 our 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 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.

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.

4.8. 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 against 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.

4.9. Reinsurance Panel

As an Insurer, we're also required 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.

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.

4.10. Debt Recovery

If you pay by direct debits and you fail to make payments, we'll appoint a debt-recovery agent to collect 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.

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

4.11. 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.

4.12. 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, audits, and monitoring.

5. How will we communicate with you?

General service communication
As an online company, we predominantly 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. All documents and formal communication are available in the customer portal.

Marketing
Our marketing communications are only sent to customers who have consented to receive these. These contain a link that'll enable you to unsubscribe at any time and you can also do this in your portal. Marketing promotes new products or promotions, offers rewards or competitions.

Telephone Calls
We record a sample of our telephone calls and a notice of this is given at the outset of a telephone call. If we contact you by telephone and there's no response, we can leave a voicemail, but we don't do this every time.

6. Cookies and Analytics

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. These cookies 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.
- *K2C* – provided by Eckoh. 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. This includes:

- *Google and Adobe Analytics* - these allow us to monitor how users interact with us. We use services provided by Google to do this including Google's Remarketing and Advertising Reporting Features. If you require further information or wish to opt out of Google Analytics Remarketing and Advertising Reporting Features, then please visit Google Opt Out
- *SessionCam* - this has been developed by SessionCam LTD. SessionCam will record mouse clicks, mouse movements and page scrolling. It captures the IP Address and Policy Reference only. The recordings are used to improve our website, detect functionality and security issues, and support us in concern and issue resolution
- *Optimise media* – Optimise help us with our digital marketing. The data collected by these cookies is anonymous
- *Optimizely* - uses persistent cookies to uniquely identify visitors, track and attribute their actions to experiments and personalisation campaigns, and deliver consistent experiences across sessions

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

7. 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.

Storing your data
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 is 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, we'll ensure that this is done securely and in compliance with all applicable transfer measures such as EU or UK approved Standard Contractual Clauses.

Aggregation, Pseudonymisation & Anonymisation
Your personal data may be anonymised. These techniques limit our ability to identify who you are. Data in this format isn't subject to the law. We also rely on pseudonymisation techniques which can allow us to process the data safely but only allow us to identify the individual using a decryption key.

Information and Cyber Security Assessments and Testing
We have a technical framework for measuring and monitoring our security environment. We conduct internal monitoring of our controls and we use external partners to help us with assessment of cyber security.

8. 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) Determining insurance risk
b) Determining 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.

b) Determining affordability

We're a consumer credit provider. This allow 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 service.

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.

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.

9. How long will we keep your information?

We'll retain your personal data for as long as is needed for us to perform our activities, meet our legal and regulatory obligations, defend, or pursue legal claims, in our legitimate interest or where fraud has been assessed.

We've agreed retention periods against our processing activities. Once that retention is met, we'll take steps to delete or anonymise the personal data.

There's information that could be retained indefinitely. This is very limited but would relate to lifelong claims, specific legal obligations, law enforcement or fraud activities.

10. Your Rights

The law provides you rights, these aren't all absolute rights and each request will be reviewed and responded to dependent on the circumstances. We'll of course do our best to help you where we can.

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

10.1. 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.

10.2. The right of access

This is more commonly known as submitting a 'data subject access request'. This can be made in writing or by telephone. 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 24/7.

When we receive a request, we may need to confirm your identity and ask for clarification of your request. 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 have 30 days to respond to your request. We can refuse to accept requests.

10.3. 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. We have 30 days to rectify the data.

10.4. 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.

We often receive requests to have payment cards removed from our records. When you purchase a policy, you're made aware that your payment card will be retained for the life of the policy for several reasons. This means we can't delete the card. There are steps we can take to ensure the card can't be used for automatic payment.

*10.5. 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.

*10.6. 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.

10.7. 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.

10.8. 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. If they can't resolve your query, then we have 30 days to provide a formal response.

11. Concerns

If you're unhappy with how we've handled your **personal data**, you can raise concerns with our Customer Services team or the **Data Protection Officer**. Each concern will be investigated and responded to within 8 weeks. You can contact our Customer Services team on 0333 043 2066 or the **Data Protection Officer** by email at DPO@1stcentral.co.uk or in writing to **Data Protection Officer**, 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.

12. 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.