Using my personal data – Home Products

Full Privacy Notice

Introduction

Thank you for choosing 1stCentral. When you applied for, interacted with our website, purchased insurance with us, you were made aware of our 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 know to fully 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 a 1stCentral 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@1st-central.com.

First Central Underwriting 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:
5.1a Waterport Place, 2 Europort Avenue, Gibraltar GX11 1AA

Contact the **Data Protection Officer** at DPO@1st-central.com.

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**.

This notice applies to all our Home insurance products. All **processing** applies generically to our products unless otherwise stated.

2. What information do we collect?

We will collect the following **personal data** about you during your application and policy 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
- Information about Your Home
    - Ownership Status
    - Occupancy
    - Home Use
    - Children
    - Pets
    - Rooms
    - Construction
    - Security
- Information about Your Contents
    - Valuables
    - Equipment
    - Personal effects
- Claims history
- Financial History
- Demographics such as lifestyle, income, and education

Sensitive personal information

- Relevant **convictions,** dates, and type
- Information pertaining to vulnerability
- Information pertaining to personal injury & lifestyle

Payment information

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

Electronic Identifiers

- IP address
- Device ID

Information you give to us on behalf of others

- Joint Policyholders – full name, date of birth, employment status and relevant **conviction** information
- Payers – the payment information, name, and address of someone paying on your behalf
- Relatives or authorised representatives – full name and date of birth
- Third Parties – if involved in a claim

Information we receive from others

- Credit score, default Information, county court judgements/IVAs and financial history
- Identity fraud markers
- Claims history

3. How will we use your information?

If you're considering buying a product or have brought a Home product, 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 activities 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 right 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 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 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, and we want to be able to reduce the risk of fraudulent policies being purchased. We use public data such as the electoral role and data sourced from credit and fraud referencing 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. <u>*Paying Online or Telephone – Deposits and in Full*</u>: 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 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. <u>*Paying Monthly*</u>: 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. You can withdraw CCA at any time. 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**.	Legitimate interest in preventing and detecting fraud and ensuring accuracy in our decision making. 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 MTA 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 date** 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 property information, - Claim history, and convictions - Occupation 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 consider privacy notices which are available in the applicable ancillary policy wording for the product you are buying. This could include **sensitive personal data.**	Necessary for entering and performance of a Contract. Substantial Public Interest – Insurance Purposes
Managing vulnerabilities	If you let us know about a vulnerability or we identify a vulnerability through our analysis, we will capture these details and use them to support you. We monitor and analyse our treatment of vulnerable customers to ensure fair outcomes are being achieved. We are also required to share details of vulnerabilities with our service providers where it is relevant, such as informing our debt recovery service if you are struggling financially. This can include **sensitive personal data**.	Legitimate Interest for meeting regulatory obligations. Substantial Public Interest – Safeguarding Economic Interest
Updating Industry Databases	We participate in industry schemes for the sharing of claims related information. When we share the data, we only provide the minimum they require for us to participate. This includes the Claims Underwriting Exchange (CUE) See section 4 of this notice for more information about these databases. We may need to share this information with law enforcement. This can include **sensitive personal data**.	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 your claim ▪ Deploying providers or services to assess, repair or act as required based on the nature of your claim. ▪ Dealing with any legal claims you or third parties may have ▪ Instructing experts or investigation services ▪ Settling any financial matters that arise from the claim ▪ Managing reinsurance We use a specialist claim handler to support us with these services and will share your information with them. 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 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 debt recovery service: This 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 share **personal data** with our legal panel. This can include **sensitive personal data**.	Legitimate Interest – recovery of monies payable under the insurance contract. 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 have a framework in place for managing fraud risk and this includes performing analysis, conducting investigations, gathering evidence, and undertaking intelligence activities. We balance our purpose with your privacy, and we consider fraud on a case-by-case basis. It isn't always possible for us to provide detailed transparency information about these activities as it could prejudice why we are doing them. ▪ 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 training colleagues to handle these activities. This can include **sensitive personal data.**	Legitimate Interest – protection of you and us Legitimate Interest – to meet regulatory obligations Substantial Public Interest – prevention and detection of unlawful acts 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 rootcauses 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**. This includes complying with: ▪ 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 do use technologies which have artificial intelligence capabilities. This includes machine learning, robotic and speech/sentiment analytics. These technologies are used to support activities in this notice. See section 9. We have a framework for management and safeguarding the use of these technologies. 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.**	Legitimate Interest – in using technology to improve processing Consent Preferences

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. 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 rootcauses ▪ Benchmarking against the wider industry ▪ Enriching the data, we hold 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 customer?

I am a witness 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** we will need will depend on the type of claim. We might need to share your information with other insurers, legal representatives as part of this process. We'll retain your information on the claim records. Our claim handlers will discuss with you the steps we need to take and what will happen. This could 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 a third party on the claim, how will you use my personal data?	We'll collect your **personal data** to: ▪ administer and manage the claim ▪ offer and provide services you are entitled to ▪ validate your identity ▪ communicate about the claim ▪ manage and resolve any concerns or complaints ▪ detect and prevent fraudulent claims We will need to share that information to provide services. Please see who we share **personal data** with and the steps we take to prevent Fraud. This could 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, email address, 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 ask you to provide information which the law classifies as **sensitive personal data** for example health information. We can also 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. Our capture of this information is limited, and we restrict how it can be used in our activities.

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 to govern the use of **sensitive personal data** or **criminal conviction data**. This information can be shared externally in limited circumstances as it relates to the activities 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 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 will not change often 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. 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. This could include sharing data in our legitimate interest. The sharing of data is assessed within data protection impact assessments.

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") 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** and the **personal data** of any Joint Policyholders to CRAs, and they'll give us information about you and them. This will include information from your application, 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 monthly, 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 https://www.transunion.co.uk/crain. 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

4.2. Insurance Industry Databases

We will pass your **personal data** to the Claims and Underwriting Exchange ("CUE"). Every insurance company is a member of the scheme. We follow membership rules and standards which are monitored by them. This scheme is provided by MIB.

The **personal data** passed to this database will include your or the Joint Policyholder name, date of birth, policy number and the date of any claims. This information is securely transmitted to ensure they're regularly kept up to date.

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

I. continuous insurance enforcement
II. law enforcement (prevention, detection and catching or prosecuting offenders)
III. providing government services or other services

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

4.3. Financial 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 annually. This means we have in place appropriate measures to protect your payment card information when processing financial transactions. 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, in order that our colleagues cannot access the data.

4.4. Fraud Prevention

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.

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 or is acting fraudulently, 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 to enrich our data and to validate no claims discounts and provide additional policy insights.

If you'd like to know more about how LexisNexis 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.

4.5. Product Partners

To provide the 1stCentral 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.

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**.

4.6. Servicing your claim

The purpose of insurance is to ensure you can access services in the event you have a claim. To do this, we use a panel of providers to help you along the way and will share your **personal data** to enable this. We will only directly share your information with our appointed claim handler who will them instruct the relevant providers based on your needs.

Due to the varying types of claims that can occur we do not list all the providers in this notice. When we discuss the steps of your claim with you, we'll let you know which provider has been instructed to help you and why.

Our panel of providers for this purpose are all subject to contracts for their services. We require that they only use your **personal data** for the purposes of providing their services. They are required to provide a comparable level of security for your **personal data**. They will in some cases be Controllers in their own right. If that is the case, you will be provided additional notices as required.

4.7. 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.

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.

4.8. Reinsurance Panel

As an Insurer, use a reinsurance panel to manage the financial risk of insurance claims. 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.

4.9. 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.

We will after a certain length of time sell our debt to our debt recovery agency. If this happens you will receive a communication advising who we have sold the debt to and what will happen.

We'll only share **sensitive personal data** if you consider yourself a vulnerable customer. This enables our colleagues who complete the debt recovery to ensure your treatment meets regulatory requirements.

4.10. 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.

4.11. 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 1stCentral.

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. 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 monitor their performance.

5. 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 Chat
We provide chat functionality on our website. This includes webchat, social channels and what's app messaging capabilities. We do have a chatbot which can support with locating information on website and help to complete online actions. We also have Colleagues available where your questions cannot be supported by our chatbot.

6. 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.
- *Egain and 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 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.

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.

8. 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. We do have information stored on servers outside of the UK and EEA.

If your information is 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 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.

9. 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 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.

The advancement of AI is part of our long term's plans and as its usage expands, we will continue to provide layered information in your experience with us. We will continue to minimise the personal data that is used and will not use capability unless we can secure that environment privately, ensuring we have the most control over the processing.

10. Wholly Automated Decision Making

To provide our services we make wholly automated decisions that will evaluate certain personal, economic, lifestyle, preference, interests, and behavioural elements about you. We make these decisions only where it is necessary to entering and performing the insurance contract, to meet regulatory obligations and prevent and detect unlawful acts. We do this using traditional modelling practices and with newer machine learning capabilities.

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 we are not required to disclose our actual algorithms or intellectual property, but we can provide meaningful logic to help you understand the decision-making process. See our website for more information on how we price our products.

a) Determining insurance risk

To consider whether we can offer you cover we will use the **personal data** we collected from you, external information about geographic locations and properties and the information you provide us about the home. All factors feed into statistical scoring models that help us determine insurance risk and ultimately the price we offer for our products.

We have underwriting criteria which sets out the minimum criteria that needs to be met for our products. For example, our buildings cover cannot be used on listed buildings due to the specialist nature of these therefore we would decline to provide a quote if you told us, you have a listed building.

Factor such as your occupation and geographical location can impact the scoring. If you are a homeworker for example, it changes the way your home is used and can increase the risk of accident and incidents. Certain geographic areas may have increased risks associated such as being near open water, near protected wildlife or are in certain surroundings that increase risk, these can increase our scoring therefore the price.

If the scoring reaches our threshold for the cover, then a consequence maybe that we don't have a product to meet your needs. This doesn't mean that you won't be insured 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 the insurance product you are buying and will complete the assessment at sale, midterm, and renewal.

b) Determining affordability

We're a consumer credit provider meaning we can offer individuals options on how they pay for their insurance. We're required by the regulators to conduct reasonable affordability and creditworthiness assessments of individuals to who we loan money for this purpose. The assessment ensures that we are a responsible lender, that you are suitable for our product and that we will not place you at risk of financial harm.
We use **personal data** we receive from credit referencing agencies, specifically your credit score, along with any payment history in this determination. If you have several defaulted accounts, we may not consider it responsible to accept a credit application from you therefore we'll offer a pay in full option only.

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.

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 and internal 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 do maintain an internal decline list. 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.

<u>Safeguarding our wholly automated decisions</u>

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.

<u>Third Parties</u>

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.

11. How long will we keep your information?

We will only permit identification of you for as long as long 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.

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 insurance up to 15 years minimally
- 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 standard retention for Home 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 and cleanse our records. We factor in the systems, usage and time to ensure that as we approach the longer retentions, we hold the bare minimum necessary to meet our obligations.

12. 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. When we receive a request, we may need to confirm your identity and ask for clarification of your request.

You can excise these rights directly to our **Data Protection Officer** by email at DPO@1st-central.com or in writing to our registered address. We have 30 days to respond to all these rights, and we can if complex extend this.

12.1. 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 short notice in your policy wording. This document is our full notice. If you would like more information on a specific topic, contact us.

12.2. 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'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.

12.3. 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.

12.4. 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.

*12.5. 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.

*12.6. 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.

12.7. 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.

12.8. 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.

13. 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.

14. 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”.
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
Conviction Data	The data relating to any motoring related convictions that the subject has disclosed on their insurance application.
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.