

# Fair Processing Notice

## Table Of Contents

<b>Table Of Contents</b>	<b>1</b>
1. About us	2
2. Personal Data that we collect	3
3. Purposes for processing	3
Insurance underwriting purposes	5
Anti-fraud purposes	5
4. Legal Basis for processing your Personal Data	6
5. How do we collect personal data?	7
6. How do we protect your Personal Data?	7
7. Who has access to your Personal Data?	8
8. Cross-border data transfers	9
9. How long do we retain your Personal Data?	10
10. Your rights regarding your Personal Data	10
11. How to exercise your data protection rights at Qover?	12

# Fair Processing Notice

Effective date: January 2024

This Fair Processing Notice (“FPN” or “Notice”) forms part of the Terms & Conditions governing our Services provided in the UK and the terms used in this Notice relate to the Information Commissioner’s Office (ICO) guidance. This Notice explains who we are, the types of Personal Data we process, how and why we collect and use the data you provide us with, with whom it is shared and how long we keep it. It also informs you of certain rights you have regarding your Personal Data under current data protection legislation. You should show this Notice to anyone covered or proposed to be covered under this policy / prospective policy.

The terms of this Notice are subjected to any additional terms, disclaimers or other contractual terms you have entered into with Qover, such as our Privacy Policy, dedicated privacy notices on the flows, and any applicable mandatory laws and regulations.

This Notice may be updated from time to time, please do check it on a regular basis [here](#).

## 1. About us

Qover S.A./N.V. (hereinafter referred to as “Qover” “we”, “us”, “our”) is a public limited liability company registered with Crossroads Bank for Enterprises (BCE/KBO) in Belgium with registration number 0650.939.878 and with registered address Rue du Commerce 31, 1000 Brussels (“Qover” “we”, “us/our”). Qover is a Belgian untied insurance agent registered with the Financial Services and Markets Authority of Belgium under the code 0650.939.878. Qover's UK branch is registered in England & Wales and with UK Establishment address: 8 Northumberland Ave – London WC2N 5BY. Authorised and regulated by the Financial Conduct Authority. Details about our authorisation can be found on the Financial Conduct Authority website (FRN 988985).

Qover as an untied agent is specialised in embedded insurance orchestration. This includes services such as distribution of insurance policies, contract management, customer support, claims and complaints management, insurance risk assessment and pricing, data analysis and reports (the “Services”).

Within this framework, Qover is the Data Controller of the Personal Data you provide us and is registered with the Information Commissioner’s Office (ICO) for the Services we provide to you. For the purpose of this Notice, “Personal Data” is any information that identifies and relates to you.

Qover has appointed a Data Protection Officer (“DPO”) for both its Belgian and the UK office. If you have any questions about how we use your Personal Data, you can contact the DPO at [privacy@qover.com](mailto:privacy@qover.com).

## 2. Personal Data that we collect

Depending on your relationship with us, for example, as a policyholder; beneficiary; claimant; legal owner, registered keeper and additional driver of a vehicle, or other person relating to our business (the “Customers” “you”, “your”), Personal Data will be collected and processed related to you or your additional driver.

We will collect Personal Data which may include your name, last name, birthdate, gender, marital and employment status, telephone number, email address, postal address, Driver’s Licence Number (DLN), additional information of risks related to your enquiry or product, such as No Claim Discount (NCD), Vehicle Registration Mark (VRM), additional drivers information, and payment details (including bank account number and sort code) which we need to offer and provide our Services or deal with a claim.

We may need to request and collect sensitive Personal Data that are necessary for providing you with our Services or for processing a claim, such as information about medical history (health data) or criminal convictions data, including driving history information, driving offences, unspent convictions, code, type and date of conviction, driving licence penalty points.

We only collect and process sensitive Personal Data where it is critical for the provision of our Services and without which the Service cannot be provided. We will therefore not seek explicit consent to process this information as the processing is legitimised by its criticality to the service provision and for reasons of substantial public interests. Possible consequences of not providing your personal data could include our inability to offer you the product or service requested, to fulfil our obligations under a contract (for example, claims management) or our breach of one or more obligations under applicable legislation (for example, accounting, tax or insurance legislation).

## 3. Purposes for processing

We process your Personal Data for specific purposes. For each processing operation, only data relevant for the purpose in question is processed.

In particular Qover processes your Personal data for the following purposes:

- Insurance underwriting purposes
- Cost calculation for the insurance coverage and provision of adequate pricing

- Evaluation of the risks to be covered and matching to appropriate insurer, policy and premium
- Preparation of insurance quotes – offers via your registration or subscription
- Personalization of our offer
- Execution and administration of your insurance contract
- Communication with you as part of our business (for example sending you important information regarding changes to our policies, terms and conditions)
- Contacting you after the registration process started: If you have already started to enter the details required for your quote, including your email address, but have not completed it, we may contact you to remind you to complete your application, provided you have consented to getting product updates and offers from us
- Contacting you to solve technical problems and fix bugs
- Contacting you in order to arrange the renewal of the insurance policy or to remind you an outstanding payment
- Management of your customer file
- Billing management
- Contacting you in order to assist you with or provide you information about your insurance policy coverage
- Customer care support and respond to your requests and enquiries
- Handling your requests related to your data protection rights
- Reviewing, investigating and handling all claims reported.
- Handling claims and reimbursement
- Claim eligibility assessment
- Investigation and resolution of complaints
- Verification of your identity when you contact us or use our Services
- Assess your eligibility for payment plans, and process your premium and other payments
- Monitor the regularity of transactions
- Improving customer satisfaction and quality of our Services
- Detection, prevention and investigation of crime, including fraud and money laundering, and analysis and management of other commercial risks. Carrying out internal and external audits
- Management of disputes with customers
- Provision of improved quality, training and security (for example, with respect to recorded or monitored phone calls to our contact numbers).
- Compliance with applicable laws and regulatory obligations (including laws outside your country of residence), such as those relating to anti-money laundering, sanctions and anti-terrorism; compliance with legal process; and

responding to requests from public and governmental authorities (including those outside your country of residence).

- Establishment, exercise, or defence of our legal claims and pursue available remedies or limit our damages.
- Recognition, exercise, defence and preservation of our legal rights or of the persons we may represent
- Conducting or participating in internal audits

In particular:

## Insurance underwriting purposes

Insurance underwriting purposes i.e. to examine the potential risk in relation to your (and/or a third party's) prospective policy so that we can:

- Provide your (or any person included on the proposal) Driving Licence Number ("DLN") to the DVLA to confirm your (or the relevant person included on the proposal) licence status, entitlement and relevant restriction information and endorsement/conviction data. Searches may be carried out prior to the date of the insurance policy and at any point throughout the duration of your insurance policy including at the mid-term adjustment and renewal stage. A search of the DLN with the DVLA should not show a footprint against your (or another relevant person included on the proposal) driving licence.
- Search your (or any person included on the proposal) 'No Claims Discount' details against a No Claims Discount database ("NCD") to obtain information in relation to your 'No Claims Discount' entitlement. Such searches may be carried out against your (or the relevant person included on the proposal) DLN, name, date of birth, gender, Vehicle Registration Mark ("VRM") and or address/postcode. For more information in relation to the NCD please visit <https://www.mib.org.uk/managing-insurance-data/mib-hub/ncd/>. A search of the DLN against the NCD should not show a footprint against your (or another relevant person included on the proposal) driving licence.
- Searches may be carried out at point of quote or point of sale and if an insurance policy is incepted during the term of your policy and renewal stage.

## Anti-fraud purposes

Anti-fraud purposes i.e. to detect and prevent fraudulent claims and/or activities by:

- Undertaking searches against your (or any person included on the proposal) DLN against details held by the DVLA to confirm your licence status, entitlement and restriction information and endorsement/conviction data. This helps insurers

check information to prevent fraud and reduce incidences of negligent misrepresentation and non-disclosure. A search of the DLN with the DVLA should not show a footprint against your (or another relevant person included on the proposal) driving licence.

- Search your (or any person included on the proposal) 'No Claims Discount' details against a No Claims Discount database ("NCD") to obtain information in relation to your 'No Claims Discount' entitlement. Such searches may be carried out against your (or the relevant person included on the proposal) DLN, name, date of birth, gender, Vehicle Registration Mark ("VRM") and or address/postcode. For more information in relation to the NCD please visit <https://www.mib.org.uk/managing-insurance-data/mib-hub/ncd/>. A search of the DLN against the NCD should not show a footprint against your (or another relevant person included on the proposal) driving licence.

## 4. Legal Basis for processing your Personal Data

The legal basis for processing your Personal Data depends on the purpose of the processing and the stakeholders involved in such processing.

In particular, providing your personal data may be necessary for:

- the execution of a contract to which you are a party (for example your insurance contract) or the execution of pre-contractual measures taken at your request (for example, in the event of a request for information for an insurance contract )
- compliance with a legal obligation applicable to Qover (for example, in matters of invoicing, fraud detection, taxation, audit by the Financial Services and Markets Authority (FSMA) and/or Financial Conduct Authority (FCA) regarding our compliance with the Insurance Distribution Directive (IDD))
- the purposes of the legitimate interests pursued by Qover (or a data recipient) provided that these interests override your fundamental rights and freedoms (for example, with regard to securing our IT systems).

In certain cases, we will ask for your free, prior and informed consent before processing some of your personal data (for example, the use of photographs of you for corporate communications purposes, or for direct marketing communication).

Also, we may process special Categories (Sensitive) Personal Data, including health data and data concerning criminal records when the processing is necessary:

- for the purposes of carrying out our legal obligations in terms of insurance law;
- for reasons of substantial public interests, namely because it is necessary for the wide range of insurance-related activities that we undertake or because it is

necessary for terrorist financing or money laundering or fraud prevention purposes or insurance purposes ([UK DPA 2018 Schedule 1 Part 2](#));

- for the establishment, exercise or defence of legal claims; or
- with your explicit consent in order to handle your claim, request or complaint.

## 5. How do we collect personal data?

We collect your personal data either directly from you or from third parties, such as our Partners or Risk Carriers. We might also collect your data from Agencies and Databases such as the Driver and Vehicle Licensing Agency (DVLA) to the extent permitted by applicable law. We might also collect your Personal Data from publicly available information (on the Internet).

We collect your Personal Data at the pre-contractual stage, during the quote process, during your insurance policy subscription for the execution of the contract and when you submit your claim form.

## 6. How do we protect your Personal Data?

We follow strict security procedures in the storage and disclosure of your Personal Data in line with industry practices.

Qover is ISO/IEC 27001 certified which verifies that Qover continuously implements technical measures to safeguard Qover's information security and Confidentiality, Integrity and Accessibility (CIA) of our customers' Personal Data. In particular, we have implemented commercially reasonable physical, organisational and technical measures in an effort to protect your Personal Data from unauthorized access, use, alteration and deletion. These safeguards may vary depending on the sensitivity, format, location, amount, distribution and storage of the Personal Data, and include measures designed to keep Personal Data protected from unauthorized access.

Access to your Personal Data is granted only on a need-to-know basis and only to persons for whom it is necessary to perform their tasks. They are bound by strict professional discretion and secrecy and shall comply with all the technical and organisational requirements laid down to ensure the confidentiality of your Personal Data.

We do our best to limit the processing of your Personal Data to what is strictly necessary and process them in compliance with our legal obligations. The type of Personal Data we request from you depends on the insurance product you are subscribing for.

Your personal data will not be used for marketing. It will only be shared within organisations involved with the administration of your insurance policy or as otherwise set out in this Notice.

We will pass details of your 'No Claims Discount' to certain organisations to be recorded on a NCD database. This will occur if information requires updating or correcting at any stage, and also at the renewal stage of your insurance policy and upon or after the cancellation of your policy prior to the expiry date.

## 7. Who has access to your Personal Data?

Depending on the type of Personal Data that is processed by Qover, only certain departments have access to your Personal Data.

Within our company, access to your Personal Data is limited to the departments and employees that are required to perform the respective purpose of processing. Furthermore, where relevant, we transfer Personal Data to our UK branch for complaints management, AML and financial sanctions monitoring.

Moreover, we will transfer your Personal Data to external recipients only insofar as this processing is necessary for purposes as described above and for which we have the respective legal basis to do so. Therefore, we may transfer your Personal Data to external third parties, including:

- service providers instructed by us (including the sub-processors of these service providers) such as in the areas of marketing, customer support, call centre, claims handling, data analytics, forms and flow builder, payment processing, AML and Fraud detection, the provision of cloud, storage and hosting services required for management and provision of our Services and the operation of Qover Website;
- Business Partners, Business Introducers;
- Risk carriers and other intervening insurance companies or insurance intermediaries and the authorities or Credit Reference Agencies (CRAs)/Credit Bureaus, or reinsurance companies, with which they share your Personal Data for fraud detection purposes or creditworthiness assessment ;
- third-party agents/brokers in connection with providing insurance quotes, binding insurance coverage, claims administration;
- Organisations and public or private authorities that help prevent and detect fraud and other related crimes, including law enforcement, policy and claims checking systems, for example, Motor Insurance Bureau (MIB) and its services, such as MyLicense, LexisNexis and its connected databases such as Motor Insurance Anti-Fraud Theft Register (MIAFTR), Motor Insurance Database (MID), Claims and

Underwriting Exchange (CUE), No claims discount (NCD) database, Driver and Vehicle Licensing Agency (DVLA) and MOT history of a vehicle, the Insurance Fraud Register, and fraud prevention agencies and databases including databases that make their data publicly available, such as on County Court Judgments (CCJ);

For details relating to information held about you by the Driver and Vehicle Licensing Agency ("DVLA") please visit [www.dvla.gov.uk](http://www.dvla.gov.uk).

For details relating to information held about you by the NCD Database please contact the MIB via email at [hubenquiries@mib.org.uk](mailto:hubenquiries@mib.org.uk).

- Regulatory Authorities and courts, such as Financial Services and Markets Authority (FSMA), Financial Conduct Authority (FCA), Autorité de protection des données (APD), the Information Commissioner's Office (ICO), the Insurance Ombudsman, national courts;
- experts, technical and legal advisors, doctors, translators, adjusters, appraisers, engineers, assessors, or other specialised consultants who might assist us with the evaluation and handling of your claims or complaints; and
- Other parties with your consent.

When these external third parties are contractually bound to us, we will ensure that they follow our documented instructions while processing your Personal Data. In particular, we ensure that they:

- process only the necessary data for the performance of their tasks and for the purpose for which they are engaged;
- undertake to treat your Personal Data securely and confidentially by implementing all the appropriate technical and organisational measures.

## 8. Cross-border data transfers

There are circumstances in which we will have to transfer your Personal Data out of the country in which it was collected for the purposes of carrying out the Services we provide to you.

In certain cases, for the purposes set out above, your Personal Data might be transferred abroad to recipients, as described above, in the so-called "Third Countries." Third Country for European Customers is a country outside EEA, while for UK customers is a country or territory outside the United Kingdom. These countries do not always provide an equivalent level of data protection and in such circumstances we take specific steps, in accordance with the applicable data protection legislation, to provide an adequate

level of protection for your Personal Data. Such transfers are subject to appropriate safeguards, including adequacy decision by the appropriate supervisory authority, the use of approved binding corporate rules or standard contractual clauses, or your consent.

## 9. How long do we retain your Personal Data?

Qover does not store your Personal Data for longer than needed for the respective purposes of processing. We only keep Personal Data for a reasonable and necessary time taking into account the purposes of the processing, our contractual obligations, mandatory legal and regulatory record-keeping requirements, and other applicable legal and regulatory obligations of limitations periods as set out by various regulators, such as FSMA, FCA.

When Personal Data is no longer needed, our company policies require that we either anonymise or aggregate the data (in which case we may further retain and use the anonymised or aggregated information for analytics purposes) or securely erase it or make it inaccessible.

We will normally keep information for no more than 7 years after termination or cancellation of a product, contract, or service we provide. In certain cases, we will keep your information for longer, particularly for any legal proceedings, where a product includes liability insurances or types of insurance for which a claim could potentially be made by you or a third party at a future date, even after your contract with us has ended.

## 10. Your rights regarding your Personal Data

Certain jurisdictions extend enhanced personal information rights to residents of or persons located in the jurisdiction. You may have some or all of the following rights in relation to the personal information we collect about or from you, depending on the jurisdiction and our reason for processing your information:

- **Right of access (article 15 EU/UK GDPR)**

You may ask us to confirm whether we are processing your Personal Data and the specific pieces of Personal Data we have collected and, if necessary, provide you with a copy of your Personal Data (along with certain other details).

- **Right to rectification (article 16 EU/UK GDPR)**

You can always ask us to rectify and complete your Personal Data that is inaccurate or incomplete.

- **Right to erasure (“Right to be forgotten”) (article 17 EU/UK GDPR)**

You may have the right to request that we delete your Personal Data, under certain conditions, such as when:

- your Personal Data are no longer necessary in regard to the purposes for which we collected them;
  - you withdraw your consent (where applicable);
  - we have legal obligation to erase your Personal Data.
- **Right to restriction of processing (article 18 EU/UK GDPR)**

You may have a right to restrict the processing of your Personal Data in certain circumstances, such as where you contest the accuracy of that Personal Data or you object to us. Please note that we process your Personal Data solely as necessary in performance of our Services, to ensure the security and integrity of the information, for the purposes of carrying out our legal obligations in terms of insurance law, for reasons of substantial public interests, for the establishment, exercise or defence of legal claims or as otherwise authorised under law or regulation. Because we do not process your Sensitive Personal Data for other purposes than what is indicated above and to the extent that such processing is necessary for the provision of our Services, you may not have the right to limit our processing of such information.

- **Right to data portability (article 20 EU/UK GDPR)**

When we process your Personal Data on the basis of your consent or for the execution of a contract, you may have the right to receive your Personal data we have obtained from you, where technically feasible, in a structured, commonly used and machine-readable format, and you may transmit your data to another controller or ask us to transfer this data to a third party of your choice.

- **Right to object (article 21 EU/UK GDPR)**

You have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you, if we based it on our legitimate interests, including profiling according to Art. 22 EU/UK GDPR.

When we process your Personal Data for direct marketing purposes (we shall ask your consent for that), you have the right to object at any time for your Personal Data to be processed (opt out of marketing communications).

- **Rights in relation to automated decision making and profiling**

Under certain circumstances, you have the right to object to being subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you.

- **Right to withdraw your consent (article 7 (3) EU/UK GDPR)**

When the processing of your Personal Data is based on a consent legal basis, you have the right to withdraw your consent at any time with effect for the future by sending us a written request at our email: [privacy@qover.com](mailto:privacy@qover.com) and we will delete your Personal Data from our repository.

Please note that if you withdraw your consent, we may not be able to process your Personal Data in order to provide you with our Services.

- **Right to lodge a complaint (article 77 EU/UK GDPR)**

If you have concerns regarding the way we process your Personal Data, you have the right to contact Qover's Data Protection Officer (DPO) by using the communication channel you prefer. For more information about how to exercise your data protection rights at Qover, please see the section below.

Further, you are entitled at any time to lodge a complaint with the responsible supervisory authority for data protection.

In Belgium, the supervisory authority is the [Belgian Data Protection Authority](#) ("Autorité de protection des données" or "APD").

In the United Kingdom, the supervisory authority is the [Information Commissioner's Office](#) ("ICO").

## 11. How to exercise your data protection rights at Qover?

To exercise any of your rights set out in the previous section, we encourage you to contact Qover's DPO by e-mail at [privacy@qover.com](mailto:privacy@qover.com) or a letter, marked for the attention of Qover's DPO to Qover's postal address:

Rue du Commerce, 31  
1000 Brussels  
Belgium

For security reasons and before providing any Personal Data to you, we may ask you to send us a written request with a proof of your identity (e.g. copy of your ID). Data such as photo and personal characteristics should be redacted on the copy.

Our use of the information on your identification document is strictly limited: we will only use the data to verify your identity and will not store them for longer than needed for this purpose.

Your request should contain a detailed, accurate description of the personal data you want access to and sufficient information about your interactions with us so that we can locate your Personal Data.

We will analyse this request and keep you informed of further developments within one (1) month from the receipt of this request, according to the article 12 (3) EU/UK GDPR.

Please note however, that the deadline may be extended by two further months where necessary, taking into account the complexity and number of the requests, as provided by the law. In such a case, we will inform you of any such extension within one month of receipt of the request, together with the reasons for the delay.

Qover will usually not charge you a fee when you exercise your rights. However, we are allowed by law to charge a reasonable fee or refuse to act on your request if it is manifestly unfounded or excessive.