

Privacy Policy

Table Of Content

| | |
|---|----|
| 1. About us | 2 |
| 2. Personal Data that we collect | 3 |
| 3. Automated decision-making and profiling | 8 |
| 4. Purposes for processing | 9 |
| 5. Legal Basis for processing your Personal Data | 11 |
| 6. How do we collect personal data? | 11 |
| 7. How do we protect your Personal Data? | 12 |
| 8. Who has access to your Personal Data? | 12 |
| 9. Cross-border data transfers | 14 |
| 10. How long do we retain your Personal Data? | 14 |
| 11. Your rights regarding your Personal Data | 14 |
| 12. How to exercise your data protection rights at Qover? | 16 |
| 13. Privacy of Minors | 17 |
| 14. Changes to this Privacy Policy | 17 |

Privacy Policy

Effective date: December 2023

This Privacy Policy forms part of the Terms & Conditions governing our Services. By using our Services means that you have read and agreed to the content anticipated in this Privacy Policy, hence we encourage you to take a moment and go through it.

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”).

For Qover your privacy is important and we want you to feel comfortable when visiting our [website](#) (“Qover Website”) or leveraging our Services.

Within this framework, Qover as a Data Controller processes your Personal Data for providing you with the Services. For the purpose of this Policy, “Personal Data” is any information that identifies and relates to you or other individuals (such as your beneficiaries or dependents).

This Privacy Policy (“Policy”) applies to any information obtained by Qover through your use of the Qover Website, Qover Flows any Qover channels of communication, such as phone calls, emails, [Contact us](#) form (collectively “Qover Channels”).

We do not sell, lease, trade or otherwise profit from your Personal Data for purposes other than our main business.

This Policy explains how and what type of Personal Data will be collected, processed and used during and following your visits to the Qover Channels, why it is collected, with whom it is shared and your rights in this regard.

This Policy does not apply to any websites controlled by third parties not affiliated with Qover that the Qover Channels may link to ("Third Party Sites"). Please review the privacy statements of Third Party Sites as Qover is not responsible for and has no influence on the content or the privacy practices of Third Party Sites.

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

We may provide privacy notices and explanations in languages other than English. If there are any discrepancies between other language versions and the English language version, the English language version is authoritative and shall prevail.

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

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.

2. Personal Data that we collect

Depending on your relationship with us, for example, as a prospect; policyholder; beneficiary; insured person benefiting under another policyholder's policy, such as close relative, or claimant; involved third-party, such as witness; commercial broker or appointed representative or main contact point; business partner (natural person), 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 and your dependents or your close relatives.

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 and may include:

- **General identification and contact information**

Full name or company name of the Customer (including dependents or representation as the case may be), residence and billing address (including, but not limited to street, street number, postal code, city, and country/region), email and phone number, date of birth, age, gender, billing address, birth place, our internal Customer ID.

- **Identification numbers issued by government bodies or agencies**

- National Identification Number (NIN), National Register Number, such as CPR;
- driving licence number (DLN), other licence number, ID or passport number and since when they are valid, if applicable;
- VAT number in case of an independent worker;
- copy of any Identification documentation (e.g. ID, passport, driving licence) if requested for claim purposes or AML monitoring (See further below).

- **Insurance Contract data**

Draft ID, Contract ID, Contract Status, Contract start date, Contract end date, Contract purchase date, additional named drivers (for UK Motor Vehicle Insurance)

- **Metadata**

Language, timezone, currency

- **Payment information and account details**

For claims reimbursement and renewal purposes, we will collect payment ID, device of conducting the payment, the four (4) last digits of your payment card, type of card and Issuer, card or account holder, card expiration date, IBAN/BIC, account number, sort code, payment method, payment status, amount.

- **Information related to the insured risk enabling us to provide you with our Services and Claim Form Data**

We will process the information necessary for us related to the insured risk enabling us to provide you with our Services. Also, we will process the Personal Data that you are submitting to us with your claim form related to information about current and/or previous claims. This information may include to the extent relevant to the risk being insured:

- Details about the covered products, including proof of purchase;
- Coverage details, cause of loss (e.g. Theft, Material Damage, Material Damage due to attempt of theft etc.);
- Information supporting your claim submission evidencing loss or damage;
- Supporting documentation for your claim including attestations, declarations, photographs and police reports evidencing theft, loss or damage, trip or event cancellation, fraudulent payment or phishing;
- Policy and claim numbers, Claim submission ID, Claim submission date;
- Type of incident, such as theft, damage, ticket/event cancellation;

- Incident description, Date and location of incident and other data related to the occurred incident included in the claim form ;
- Only for bike insurance, Information regarding your bike (such as GPS, brand GPS, invoice, markings, special number, brand of marking, bike marking ID, purchase invoice of your bike, location of your stolen/damaged bike, brand of locker);
- Only for bike insurance, location data, namely the last location of your bike when it was stolen that you provide us for, as well as any other related location data that we receive from our Partners in case of an incident and only on a need-to-know basis;
- Only for trip and event cancellation coverages: Trip or event details;
- For purchase protection coverages: Details about the covered product, including proof of purchase, information about the retailer;
- For bill protection coverages: bills data related to rent, utilities (such asb. Utilities (Electricity, Gas, Water, Internet, mobile phone), groceries, travel
- For Motor Vehicle Insurance or Third - Party Liability (TPL): Vehicle Identification Number (VIN), licence plate number or Vehicle Registration Number (VRN), car model, brand, data related to previous accident, condition of car (new/used), capacity of your car as being stolen, No Claims Discount (NCD), licence validity date, licence type, MOT history of a vehicle, vehicle registration date, length of time owned (vehicle), declared mileage, vehicle usage (private/business), legal owner and registered keeper of the vehicle, count of all Insolvencies in last 6 years for individual, if applicable, ;
- For home insurance: Property information, such as your status as tenant, owner or roommate, property type (apartment, home, other), accommodation location, monthly rent;
- Data related to your family composition, such as marital status, number and names of dependents/family members;
- Employment status: job title, industry, date of recruitment, employer, fired from a permanent employment or job loss, proof of income if applicable;
- Other insurance you hold and for how long or previous insurance information about the insurer, contract number, whether your insurer cancelled or terminated your motor insurance policy or subjected you to any special conditions;
- Number of claims in the 5 past years;
- Any other data you voluntarily communicate to us.

- **Data related to request or complaints**

Request or complaint email or form

- **Content of electronic communications and telephone recordings**

Qover processes any information you provide to us when you communicate with us via phone, SMS, chat, email, or any other channel of communication, including customer support service tickets. We store recordings of telephone conversations, emails, chats, SMS, for training purposes, for the purpose of monitoring the quality of our Service and to retain proof relating to our legal obligation or lawful commercial transactions to the extent permitted by applicable law.

- **Information to investigate or prevent crime, including fraud and money laundering**

General identification and contact information is being processed in order to investigate or prevent crime, including fraud and money laundering, and monitor Financial Sanctions. We might process individual information about fraud convictions, allegations of crimes and sanctions details received from various anti-fraud and sanctions databases, or regulators or law enforcement agencies. Also, we might ask for a copy of any Identification documentation (e.g. ID, passport, driving licence) and all the information therein.

- **Qover Website related information**

Information related to the operation of and use of Qover Website and information collected through cookie or other tracking technologies, which may include log-in credentials, IP addresses, domain names, browser versions and operating system, traffic data, the resources you access, user's web session and other Site-related information. For more information, please visit our [Cookie Policy](#).

- **Registration and quote information**

Within the scope of our Services, we offer you the option to register. This is necessary to obtain a cost calculation for the desired insurance coverage and an offer to execute an insurance contract ("quote"). For this, we request your name, email address, and further details about you and in connection with the risk to be insured. This is necessary to establish insurability or, as applicable, the level of potential insurance premium for you. The processing of this data is necessary in each case to prevent fraud, make the desired quote available to you for cost calculation and to be able to send you an appropriate offer by email, if necessary, with the provision of further information on the execution of an insurance contract. The processing therefore serves as preparation for entering into a possible insurance contract between us.

- **Marketing preferences, customer feedback and survey responses**

If you have agreed to receive product updates and offers from us, we will process your email address, and potentially, information included in your account, based on your corresponding consent, in order to be able to send you any marketing communication and information with regard to our Services, offers, and activities (contest or prize draw or other sales promotion) in the areas of insurance

We also may periodically obtain both personal and non-personal information about you from our business partners and other independent third-party sources, through your interactions and/or use of our Services in order to assess the quality of our Services. Your consent may be obtained by us or on our behalf by our partners.

You can always request to unsubscribe from further non-essential emails from us.

Also, we may process your Personal Data in case you consented to participate in a voluntary survey organised by us.

- **Social media accounts**

We may receive certain Personal Data about you when you use our Social Media Pages, including your social media account ID and profile picture. If you select to connect any of your other social media accounts to your account(s), personal information from your other social media account(s) will be shared with us, which may include Personal Data that is part of your profile relating to those accounts or your connections' or followers' profiles.

- **Special Categories (Sensitive) Personal Data, including Criminal Records Data**

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

(a) for the purposes of carrying out our legal obligations in terms of insurance law;

(b) 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](#));

(c) for the establishment, exercise or defence of legal claims; or

(d) with your explicit consent in order to handle your claim, request or complaint.

The following data may be processed:

- **Health data**, including health status, such as sickness, disability, physical, mental and medical condition, bodily injuries, medical history and

procedures, causes of death, relevant personal habits (such as smoking, alcohol consumption)

- **Criminal Records Data – criminal convictions**, including driving history information, driving offences, unspent convictions, code, type and date of conviction, driving licence penalty points (for UK Motor Vehicle Insurance)

Before you provide us with Special Categories of Personal Data and Criminal Records Data about a person other than yourself, you agree to notify such person of our use of their personal information and, if requested by us, to obtain their consent to our use of their Special Categories of Personal Data and Criminal Records Data (for example, by requiring the individual to sign a consent form).

3. Automated decision-making and profiling

We do not profile and make any automated decisions for the users of our Website.

However, only under certain circumstances and objective criteria, we utilise automated decision-making in connection with the provision of our Services or the compliance with our legal obligations. In particular, we will use automated decision-making, including profiling, to evaluate the information you provide to us during the quote process to calculate your individual risk profile in order to determine whether we can extend insurance coverage to you, and if so, what your insurance coverage limits and premiums will be, or to process claims you submit (e.g. refusal of your claim) or to prevent and detect fraud, or to execute standard contract lifecycle modifications on your behalf (e.g. cancelling a contract upon receiving a valid request from you).

Depending on the purposes pursued by automated decision making or profiling, we use as legal basis either (a) the necessity for the performance of the contract binding us or for the implementation of pre-contractual measures at your request prior entering to a contract with us or (b) our legal and regulatory obligation or (c) your explicit consent.

Regarding the assessment of the premium and coverage, we use objective “segmentation criteria” which meet all applicable legal requirements. These criteria vary according to the product and stem from the statistical observation that they have an impact on the occurrence and/or severity of a claim. Regarding the processing of your claim or execution of contract lifecycle modification, we use a deterministic and rule-based assessment in order to make an automated decision or to submit this for human analysis, by verifying information you provided against your coverage limits and exclusions.

In case that we rely on solely automated processing, we ensure that we have an appropriate legal basis for this processing activity and we implement all the suitable

measures to safeguard your rights, freedoms and interests. In particular, we use only anonymous or pseudonymized data for profiling, if possible, and we safeguard all your rights, including your right to easily obtain human intervention and explanation, to express your point of view and to contest the decision.

By applying for insurance or submitting your claim, you acknowledge that you understand that automated decision-making or profiling may be used as described above in this Policy.

4. 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:

- 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
- 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
- Retrieval of your stolen item (e.g. bike)
- 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
- Improving Qover Website experience for our customers
- Conducting surveys, such as satisfaction surveys
- Data analysis and statistical evaluation and compilation
- Analysing client loss data history to review our products
- 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).
- Provision of marketing or promotional information to you (including information about our new products and / or services or other products and services offered by selected third-party partners) in accordance with preferences you have expressed.
- Sending you our newsletters
- Allow you to participate in contests, prize draws, games, challenges and similar promotions, and to administer these activities. Some of these activities have additional terms and conditions, which could contain additional information about how we use and disclose your Personal Data, so we suggest that you read these carefully.
- 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

Possible consequences of not providing your personal data could include our inability 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).

5. 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.

6. 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.

7. How do we protect your Personal Data?

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.

However, as effective as our security measures are, no security system is impenetrable and no method of transmission over the Internet, or method of electronic storage, is fully secure. Hence, we cannot guarantee that information you supply will not be intercepted while being transmitted to us over the Internet.

8. 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);
- Only for Motor Vehicle insurance products, local authorities and insurance associations for plate registration, for example: Motor Data Solutions (MDS), German Insurance Association (GDV), RDW, Stichting EPS, Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF);
- 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.

9. 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.

10. 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.

11. 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 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").

12. 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 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.

13. Privacy of Minors

Our Services are not directed to individuals under the age of eighteen (18). When a minor is indirectly covered by the insurance policy, as a dependent of an insured, we ensure that its authorised representative provides validly any Personal Data through the Qover Channels.

14. Changes to this Privacy Policy

We review this Privacy Policy regularly and reserve the right to modify or adapt the provisions of this Policy at any time to take account of changes in our business and legal requirements. If we make changes to this Privacy Policy, we will update the "Effective Date" at the top of this document. The changes will be applicable at the time of the publication on our Website. As such, we advise you to consult the most recent version of this Policy.