

PRIVACY POLICY

Brooks Braithwaite & Company Limited strives to protect the privacy and the confidentiality of Personal Data that the company processes in connection with the services it provides to clients and individuals' use of the our websites. Brooks Braithwaite's services consist primarily of risk consulting and insurance broking, which enable the consideration of, access to, administration of, and making of claims on, insurance and consultancy, advice and support surrounding employee health and benefits and risk management.

To arrange insurance cover and handle insurance claims, Brooks Braithwaite and other participants in the insurance industry are required to use and share Personal Data.

During the insurance lifecycle Brooks Braithwaite will receive Personal Data relating to potential or actual policyholders, beneficiaries under a policy, their family members, claimants and other parties involved in a claim. Therefore references to "individuals" in this notice include any living person from the preceding list, whose Personal Data Brooks Braithwaite receives in connection with the services it provides under its engagements with its clients. This notice sets out Brooks Braithwaite's uses of this Personal Data and the disclosures it makes to other insurance market participants and other third parties.

Identity of controller and contact details

Brooks Braithwaite & Company Limited of 5 Grange Court, The Limes, Ingatestone, Essex CM4 0GB is the controller in respect of the Personal Data it receives in connection with the services provided under the relevant engagement between Brooks Braithwaite & Company Limited and its client.

Personal information that we process

We may collect and process the following Personal Data:

Individual details - name, address (and proof of address), other contact details (e.g. email and telephone details), gender, marital status, family details, date and place of birth, employer, job title and employment history, relationship to the policyholder, insured, beneficiary or claimant;

Identification details - identification numbers issued by government bodies or agencies (e.g. depending on the country you are in, social security or national insurance number, passport number, ID number, tax identification number, driver's licence number);

Financial information - payment card number, bank account number and account details, income and other financial information.

Insured risk - information about the insured risk, which contains Personal Data and may include, only to the extent relevant to the risk being insured:

- Health data - current or former physical or mental medical conditions, health status, injury or disability information, medical procedures performed, relevant personal habits (e.g., smoking or consumption of alcohol), prescription information, medical history;
- Criminal records data - criminal convictions, including driving offences; and
- Other special categories of Personal Data - racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning an individual's sex life or sexual orientation.

Policy information - information about the quotes individuals receive and the policies they obtain;

Credit and anti-fraud data - credit history and credit score, information about fraud convictions, allegations of crimes and sanctions details received from various anti-fraud and sanctions databases, or regulators or law enforcement agencies;

Previous claims - information about previous claims, which may include health data, criminal records data and other special categories of Personal Data (as described in the Insured Risk definition above);

Current claims - information about current claims, which may include health data, criminal records data and other special categories of Personal Data (as described in the Insured Risk definition above);

Marketing data – We will not collect or use data for marketing purposes without specific written consent of the individual

Website and communication usage - details of your visits to our website and information collected through cookies and other tracking technologies, including, but not limited to, your IP address and domain name, your browser version and operating system, traffic data, location data, web logs and other communication data, and the resources that you access.

Where we collect such information directly from individuals, we will inform them of whether the information is required and the consequences of not providing it on the relevant form.

Sources of personal data

We collect and receive Personal Data from various sources, including (depending on the service provided and country you are in):

- Individuals and their family members, online or by telephone, or in written correspondence;
- Individuals' employers or trade or professional associations of which they are a member;
- In the event of a claim, third parties including the other party to the claim (claimant/ defendant), witnesses, experts (including medical experts), loss adjusters, lawyers and claims handlers;
- Other insurance market participants, such as insurers, reinsurers and other intermediaries;
- Credit reference agencies (to the extent Brooks Braithwaite is taking any credit risk);
- Anti-fraud databases and other third party databases, including sanctions lists;
- Government agencies, such as vehicle registration authorities and tax authorities;
- Claim forms;
- Open electoral registers and other publicly available information;
- Business information and research tools;
- Companies House Beta
- Third parties who introduce business to us; and

How we use and disclose your personal data

In this section, we set out the purposes for which we use Personal Data, explain how we share the information, and identify the “legal grounds” on which we rely to process the information. These “legal grounds” are set out in the General Data Protection Regulation (the GDPR), which allows companies to process Personal Data only when the processing is permitted by the specific “legal grounds” set out in the GDPR.

Consent

In order to facilitate the provision of insurance cover and administer insurance claims, unless another legal ground applies, we rely on the data subject’s consent to process special categories of Personal Data and criminal records data, such as medical and criminal convictions records, as set out in the table above and for profiling as set out in the next section. This consent allows us to share the information with other insurers, intermediaries and reinsurers that need to process the information in order to undertake their role in the insurance market (which in turn allows for the pooling and pricing of risk in a sustainable manner).

The affected individual’s consent to this processing of special categories of Personal Data and criminal records data may be necessary for Brooks Braithwaite to be able to provide the services the client requests.

Where you are providing us with information about a person other than yourself, you agree to notify them of our use of their Personal Data and to obtain such consent for us.

Individuals may withdraw their consent to such processing at any time by contacting the Data Protection Officer using the contact details in the Questions, Requests or Complaints section below. However, doing so may prevent Brooks Braithwaite from continuing to provide the services to the relevant client. In addition, if an individual withdraws consent to an insurer’s or reinsurer’s processing of their special categories of Personal Data and criminal records data, it may not be possible for the insurance cover to continue.

Profiling and automated decision making

Insurance premiums are calculated by insurance market participants benchmarking clients' and beneficiaries' attributes as against other clients' and beneficiaries' attributes and propensities for insured events to occur. This benchmarking requires Brooks Braithwaite and other insurance market participants to analyse and compile information received from all insureds, beneficiaries or claimants to model such propensities. Accordingly, we may use Personal Data to both match against the information in the models and to create the models that determine the premium pricing in general and for other insureds. Brooks Braithwaite and other insurance market participants may use special categories of Personal Data and criminal records data for such modelling to the extent it is relevant, such as medical history for life insurance or past motor vehicle convictions for motor insurance.

Insurance market participants use similar predictive techniques to assess information that clients and individuals provide to understand fraud patterns, the probability of future losses actually occurring in claims scenarios, and as set out below.

We use these models only for the purposes listed in this Privacy Notice. In most cases, our staff make decisions based on the models.

- **Automated broking platform**

Where clients use the automated broking platform, insurance quotations are offered entirely by matching whether the attributes that the client has provided meet the criteria set by the insurers, which determines (a) whether a quotation will be made; (b) on what terms; and (c) at what price. Each insurer will use different algorithms to determine their pricing, and clients must consult each insurer's privacy policy for further details. Our platform merely queries whether attributes of potential insureds satisfy insurers' models and then returns the results. If the potential insured's attributes do not satisfy insurers' models, the quotation request is referred for review by a team with underwriting authority. Insurers also apply fraud prediction algorithms to the information clients provide to assist in detecting and preventing fraud.

These partially automated processes may result in a client not being offered insurance or affect the price or terms of the insurance.

Clients may request that we provide information about the decision-making methodology and ask us to verify that the automated decision has been made correctly. We may reject the request, as permitted by applicable law, including

when providing the information would result in a disclosure of a trade secret or would interfere with the prevention or detection of fraud or other crime.

Safeguards

We have in place physical, electronic, and procedural safeguards appropriate to the sensitivity of the information we maintain. These safeguards will 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 unauthorised access. If appropriate, the safeguards include the encryption of communications, firewalls, access controls, separation of duties, and similar security protocols. We restrict access to Personal Data to personnel and third parties that require access to such information for legitimate, relevant business purposes.

Limiting collection and retention of personal information

We collect, use, disclose and otherwise process Personal Data that is necessary for the purposes identified in this Privacy Notice or as permitted by law. If we require Personal Data for a purpose inconsistent with the purposes we identified in this Privacy Notice, we will notify clients of the new purpose and, where required, seek individuals' consent to process Personal Data for the new purposes.

Our retention periods for Personal Data are based on business needs and legal requirements. We retain Personal Data for as long as is necessary for the processing purpose(s) for which the information was collected, and any other permissible, related purpose. For example, we retain certain transaction details and correspondence until the time limit for claims arising from the transaction has expired, or to comply with regulatory requirements regarding the retention of such data. When Personal Data is no longer needed, we securely destroy the data.

Accuracy, accountability, openness and your rights

We strive to maintain Personal Data that is accurate, complete and current.

Questions regarding Brooks Braithwaite privacy practices should be directed to the Data Protection Officer using the contact details at the Questions, Requests or Complaints section below.

Under certain conditions, individuals have the right to request that Brooks Braithwaite:

- provide further details on how we use and process their Personal Data;
- provide a copy of the Personal Data we maintain about the individual;
- update any inaccuracies in the Personal Data we hold;
- delete Personal Data that we no longer have a legal ground to process; and
- restrict how we process the Personal Data while we consider the individual's enquiry.

In addition, under certain conditions, individuals have the right to:

- where processing is based on consent, withdraw the consent;
- object to any processing of Personal Data that Brooks Braithwaite justifies on the "legitimate interests" legal grounds, unless our reasons for undertaking that processing outweigh any prejudice to the individual's privacy rights; and
- object to direct marketing (including any profiling for such purposes) at any time.

These rights are subject to certain exemptions to safeguard the public interest (e.g., the prevention or detection of crime) and our interests (e.g., the maintenance of legal privilege). We will respond to most requests within 30 days.

If we are unable to resolve an enquiry or a complaint, individuals have the right to contact the UK data protection regulator, the Information Commissioner's Office.

Questions, requests or complaints

To submit questions or requests regarding this Privacy Notice or Brooks Braithwaite's privacy practices, please write to the Data Protection Officer at the following address:

The Data Protection Officer
Brooks Braithwaite & Co Ltd
5 Grange Court
The Limes
Ingatestone
Essex CM4 0GB
Phone: 01277 354573
Email: 03.05bb-chequers@btconnect.com

Links to third party websites

Our websites may contain links to other third party websites. If you follow a link to any of those third party websites, please note that they have their own privacy policies and that we do not accept any responsibility or liability for their policies or processing of your personal information. Please check these policies before you submit any personal information to such third party websites.

Changes to this privacy notice

This Privacy Notice is subject to change at any time. It was last changed on 05.04.18. If we make changes to this Privacy Notice, we will update the date it was last changed. Where we have an engagement with you, we will notify you of any changes we make to this Privacy Notice in accordance with the notice provisions in the terms of our engagement. In other circumstances, we will publish the revised Privacy Notice on our website.