Brown & Brown, Inc. Global Privacy Statement

Last updated: October 1, 2024

Brown & Brown, Inc., and its subsidiaries and affiliates worldwide (collectively, "Brown & Brown", the "Company", "we", "us", "our"), take your privacy seriously. This Global Privacy Statement ("Statement") describes how we collect, use, disclose, transfer across borders, and otherwise handle (collectively, "process") your personal information. This Statement also describes your choices regarding our handling of your personal information and how to make those choices, how we safeguard your personal information, and how you may contact us regarding our privacy practices.

The term "personal information" as used in this Statement means, unless specified otherwise, any information related to or about an identified or identifiable natural person.

This Statement contains the following sections:

1. Scope of this Statement

You may interact with Brown & Brown online and offline for a variety of reasons. This section explains when the Statement applies to Brown & Brown's processing of your personal information.

Brown & Brown as Data Controller: Unless stated otherwise, this Statement applies to any personal information you provide to Brown & Brown and any of your personal information we collect when you:

- visit or use our websites or applications (together the "Site")
- visit a Brown & Brown office or other physical location
- attend events or seminars hosted by Brown & Brown
- request a service from us or use other services that refer to or link to this Statement (each, a "Service").

This Statement also applies to personal information Brown & Brown may collect from or about the corporate representatives of clients, vendors, suppliers, business partners, and others for the purposes of conducting our own business, such as contracting and invoicing. This personal information generally is limited to contact details and other limited information necessary to complete business transactions ("Business Contact Information").

Identification of the Data Controller: The Brown & Brown entity whose website or physical location you visit, event you attend, or Service you use also is responsible for the processing of your personal information collected in relation to the visit, event, Service, or business relationship ("data controller").

A full list of the Brown & Brown entities and their contact details is available ***here***.

This Statement does not apply to the processing of your personal information described below:

Brown & Brown as Data Processor: At times, Brown & Brown may collect and otherwise process personal information in our capacity as a data processor, meaning that we handle your personal information only on our client's behalf and in accordance with their instructions. This Statement does not apply to Brown & Brown's processing of personal information as a data processor. For information about this processing of your personal information, please refer to the website of the Brown & Brown client on whose behalf Brown & Brown is providing the service.

Brown & Brown as Employer: This Statement does not apply with respect to the personal information processed by Brown & Brown in our capacity as an employer, including the personal information of job applicants who apply for employment with Brown & Brown or the Company's current or former employees or independent contractors. Brown & Brown maintains separate policies, as required by law, with respect to the Company's processing of personal information in its capacity as employer.

Third-Party Sites: The Site may include links to, and plug-ins from, sites or applications operated by third parties ("Third-Party Sites"). Brown & Brown does not control any Third-Party Sites and is not responsible for any personal information they may collect. The information collection practices of Third-Party Sites are governed by their privacy policies. If you choose to enter any Third-Party Site from the Site, please refer to that site's privacy policy to learn more about that site's processing of your personal information.

Return to the top.

2. Your Consent

"Consent" means any freely given, specific, informed and unambiguous indication of your wishes by which you, by a statement or by a clear affirmative action, indicate your unambiguous agreement to the processing of your personal information.

By providing your personal information to Brown & Brown as data controller, you consent to Brown & Brown's processing of your personal information as described in the Statement, as it may be modified from time to time. You also have the right to withdraw your consent at any time. As our business evolves, this Statement may change, so check back to this page periodically to make sure you understand how your personal information will be handled. Where processing of your data requires explicit consent, this will be obtained directly from you prior to proceeding.

Please understand that you are not obliged to provide your personal information to the Company. However, if you do not provide your personal information, or otherwise do not consent to the processing of your personal information or withdraw your consent to the processing, the Company may not be able to provide you with certain Services and may be required to terminate the Services currently provided to you.

Where applicable law requires a lawful basis for collecting, using and otherwise processing your personal information and you do not consent or you withdraw your consent, the Company relies on the following alternative grounds as applicable:

- as necessary to enter into a contract for Services with you, and to perform our obligations under that contract;
- as required to fulfill the Company's legal obligations;
- as necessary to exercise the Company's rights or defend against legal claims;
- where applicable, as necessary for the Company to pursue our legitimate business interests, such as managing our relationship with our clients, suppliers, and you, maintaining our business records, and improving our products and Services.

Before collecting your sensitive personal information, we will, when required by applicable law, provide you with a separate notice and, if the collection is not required by applicable law, request your explicit consent whenever legally required to do so.

Return to the top.

3. Personal Information We Collect

The types of personal information we collect will vary depending upon the reason that you are interacting with us and may include the following:

- **Contact details:** such as your name, email, mailing address, and phone number.

- **Identification details:** Identification numbers issued by government bodies or agencies, including your Social Security number, national insurance number, passport number, tax identification number, state ID card number, driver's license number, photographs, or audio or video recordings of you, for example, when you call one of our service centers or visit one of our physical locations.

- **Demographic details:** such as your date of birth, age, gender, marital status, and insurance requirements.

- **Employment information:** such as employer, job title, employee number, employment status, salary, ethnicity, employer history, employment benefits, and family details, including their relationship to you.

- **Health information:** such as medical records, health status, injury or disability information, medical treatment, personal habits (for example, smoking), prescription information and medical history.

- **Benefits information:** such as benefit elections, pension entitlement information, date of retirement and any relevant matters impacting your benefits, *e.g.*, voluntary contributions, pension sharing orders, tax protections or other adjustments.

- **Financial information:** such as bank account number or other financial account number and account details, credit history and bankruptcy status, salary, bonus payments, benefits and entitlement data, and national insurance contributions details, only as necessary to provide our Services.

- **Claims details:** Information about previous and current insurance claims, (including other unrelated insurances), which may include data relating to claims concerning you or your employer's insurance policy.

- **Marketing and communications preferences:** such as interests and preferred language. To improve our marketing communications, we may also collect information about interactions with, and responses to, our marketing communications.

- **Events information:** such as information about food allergies or dietary restrictions along with feedback forms when registering for or attending in-person events.

- **Background checking information:** such as inclusion on a sanctions list or a public list of disqualified directors, the existence of previous or alleged criminal offences, or confirmation of clean criminal records, information in relation to politically exposed persons ("PEPs"), only where this information is (i) applicable in the context of the Service you have requested; and (ii) we have obtained your consent, as appropriate.

- **Comments, feedback or other information provided to us:** such as social media interactions with our social media presence, comments provided on feedback forms or surveys and questions or information sent to our support services.

- **Account login credentials:** such as username and password, and security information related to your account with us.

- **Payment information:** such as credit or debit card number and bank account details to facilitate payment on behalf of insurers.

- **Driving history, certifications and insurance details:** such as driving license details, the period for which a license has been held, existing and previous insurance policy details, previous accident and claims history and details of any motoring convictions, only as part of your application for and administration of the Service to be provided.

- **Telephone recordings:** Recordings of telephone calls with our representatives and call centers.

- **Photographs and video recordings:** Images (including photographs and pictures) or video recordings created in connection with our insurance or other business activities, including for claims assessment, administration and settlement, claim disputes, or for other relevant purposes as permitted by law, as well as CCTV recordings captured by equipment on our premises.

- **Online information:** Such as device, computer and connection information, device location information, and data collected during use of our website.

- **Business Contact Information:** Such as your name, employer, job title, business mailing address, business email address, business phone number, and other information necessary for the administration of the relationship between Brown & Brown and your employer.

Brown & Brown may collect sensitive personal information (such as health information and criminal history information) as described above. We do so only to the extent necessary for the provision of Services and only if and to the extent permitted by applicable laws. Whenever legally required to do so, we will provide you with a separate notice and request your consent before collecting your sensitive personal information.

If you provide us with personal information relating to other people (*e.g.,* your spouse, civil partner, dependents, beneficiaries, etc.), we will process that information in accordance with this Statement. You are responsible for the accuracy of such information and for ensuring that those people are informed that you provided their personal information to Brown & Brown and that we will process their personal information in accordance with this Statement.

Automated Collection of Information on the Site

When you browse our Site, we may collect information automatically through technology to help enhance our ability to serve you. This may include: the name of the domain and host from which you access the Internet; the Internet protocol (IP) address of the computer you are using; the browser software you use and your operating system; the date and time you access our Site; and the Internet address of the site from which you linked directly to our Site.

We may use this information only as anonymous aggregate data to determine the number of visitors to different sections of our Site, to ensure the Site is working properly, and to help us make our Site more useful. For example, we may use your IP address to assist in correcting server problems and to administer our Site. Additionally, we may use this information for statistical purposes, such as determining user demographics for advertising purposes. We do not use this information to track or record information about individuals.

Cookies: Cookies are small pieces of data stored by your internet browser on your computer's hard drive. They cannot be used to collect data from your hard drive, obtain your e-mail address or personal information about you.

If you are browsing our Site, we may also use cookies or similar mechanisms to help us measure the number of visits, time spent, pages viewed and other statistics about traffic to our Site. We may also use cookies provided by Google Analytics for collecting website analytics and could use the information set forth above. For more information on Google Analytics, and how it collects and processes data, go to: https://www.google.com/policies/privacy/partners/.

You may set your browser to notify you when you receive a cookie or to prevent cookies from being sent. Please note that when you block the acceptance of cookies you limit the functionality we can provide when you visit our Site. For more information about cookies and other technologies we use on the Site, please review our Cookies Policy.

Do Not Track Setting: The Site does not track your online activities over time and across websites or online services on an individually identifiable basis, and we do not allow third parties to use our Site to track your activities over time or across other websites. Your web browser may have settings that allows you to transmit a "Do Not Track" signal when you visit various websites or use online services. Like many websites, the Site is not designed to respond to "Do Not Track" signals received from browsers. To learn more about "Do Not Track" signals, go to: https://allaboutdnt.com/.

Return to the top.

4. Sources of Personal Information

We may collect personal information about you from the following sources:

- **Directly from you:** We collect personal information about you when you submit an application for a Service, use a Service, visit our Site, register for or attend an event, or otherwise communicate directly with us.

- **From your employer or representative:** We may obtain personal information about you from your employer or the company with which you are affiliated in order to provide Services to them and/or manage your access to such Services.

- **From a third party acting on your behalf:** We may collect personal information from your family members, financial advisor or representative.

- **From insurance carriers and third-party agent/brokers:** In the event of a claim, we will receive information about you from third parties, including the other party to the claim (claimant/defendant), witnesses, experts (including medical experts), loss adjusters, attorneys, and claims handlers.

- **From automated technologies:** We may obtain personal information about you through automated technologies, such as cookies on our Site (as described in more detail in Section 3, above), or from surveillance or recording technologies, such as video surveillance in Company facilities.

- **From acquired entities:** If we acquire an entity as part of a corporate transaction, we may obtain personal information about you from that entity.

- **From other third parties:** We may obtain your personal information from credit reference agencies, anti-fraud databases, sanctions lists, court judgements and other judicial databases, government agencies, open electoral register and any other publicly available data sources.

Return to the top.

5. How We Use Personal Information

Depending on the nature of your interaction with Brown & Brown (e.g., as a policyholder, website user, business contact), we may use personal information about you for the following purposes:

Providing Services to You or on Your Behalf:

- To arrange insurance coverage (issue quotations, inception of a Service, renewals)
- To administer policies and process claims
- To make assessments and decisions, including whether to pay your claim or pursue any losses against you or a third party, provide you with our products and Services, on what terms and whether you are eligible for a payment plan
- To process payments when you purchase a product or Service and any refunds
- To collect, forward and refund premiums
- To facilitate premium finance arrangements
- To conduct credit assessments and other background checks
- To provide other Services to you, at your request or at the request of a third party acting on your behalf

Communicating With You:

- To communicate with you about our products and Services
- To operate, assess activity on, and improve the Site and related Services
- To conduct marketing
- To allow members of the Brown & Brown family of companies to notify you of certain products or Services offered by them

Managing Our Business:

- To process business-related transactions, such as the purchase of products or services from vendors or suppliers
- To manage relationships with third parties (e.g., brokers and vendors)
- To facilitate business transfers to successors of the business in the event of sale, reorganization, or other corporate transaction, including due diligence and planning

Complying With Legal Obligations and Protecting Ourselves:

- To comply with applicable legal, regulatory and professional obligations, including cooperating with regulatory bodies and government authorities
- To comply with law enforcement requests
- To exercise and defend ours, yours, or applicable third parties' legal rights
- To undertake anti-fraud, sanction, anti-money laundering and other checks to protect against fraudulent, suspicious or other illegal activities
- To conduct compliance/security monitoring and screening
- To conduct internal investigations into alleged violations of Company policy or applicable legal requirements
- To monitor and ensure the safety and security of our premises, property, employees and visitors
- To engage in other activities we believe necessary to meet legal, security, and regulatory requirements

Improving our Services:

- To conduct research and statistical analysis
- To build databases related to the Services for use by us and others with which we may share information
- To improve our products and Services
- To provide staff training, including by recording and monitoring telephone calls
- To maintain information security
- To conduct customer analysis, market research and focus groups, including customer segmentation, campaign planning, creation of promotional materials, gathering customer feedback, and conducting customer satisfaction surveys
- To manage concerns and complaints, including to allow us to respond to any current complaints or concerns you or others might raise later, for internal training and monitoring purposes and to help us to improve our complaints handling processes.

No Automated Decision Making

The Company does not use the personal information collected for automated decision-making, including profiling, that produces legal effects or similarly significantly effects on Non-U.S. Residents.

Return to the top.

6. How We Disclose Personal Information

We do not, and will not, sell your personal information or disclose it to third parties for cross-context behavioral advertising ("sharing"). We may disclose personal information to the following categories of third parties for the following purposes:

- **Service Providers**: We may disclose your personal information to service providers to provide services to us or on our behalf and to assist us in meeting our business needs and contractual and legal obligations — for example, to host all or portions of the Site, to process payments, or to conduct credit, background or other screening. Service providers will be permitted to process your personal information only for the purpose(s) for which it was disclosed to them and in accordance with the Company's instructions.

- **Professional Advisers and Related Third Parties:** For example, we may disclose personal information to lawyers to assist us with legal compliance, auditors, accountants, consultants, insurance carriers, reinsurers, intermediaries, and third-party agents/brokers to assist us in providing Services to you or in otherwise conducting our business.

- **Corporate Affiliates**: Your personal information may be disclosed to other companies within the Brown & Brown family of companies, for example, to provide you with our products and Services or to provide you with information about their products and Services.

- **Government Authorities or Administrative Agencies:** We may disclose your personal information, for example, to law enforcement or regulatory bodies or tax authorities.

- **Other Third Parties:** We may disclose your personal information to other third parties;

    - **When Required By Law**: for example, when we respond to subpoenas, court orders, legal process, or discovery requests in civil litigation.

    - **To Protect Rights, Property or Safety**: If we believe that your actions violate applicable law, or threaten the rights, property, or safety of the Company, our clients, or others.

    - **In Corporate Transactions**: We may disclose and transfer your personal information, including to a subsequent owner or co-owner, of our business, including in connection with a corporate merger, consolidation, bankruptcy, the sale of all or substantially all of our membership interests and/or assets, or other corporate change.

The Company will make the disclosures described above only as permitted by applicable laws.

Return to the top.

7. Cross-Border Data Transfers

Due to the global nature of our business and for the purposes set forth above, we may transfer personal information to parties located in countries other than the one where you reside, including in the United States. For example, we may transfer personal information internationally to our subsidiaries, affiliates, service providers, business partners and governmental or public authorities in another country in connection with the performance of our Services. The laws of these countries may provide a different level of protection for personal information than the country where you reside.

We will, when required by applicable law, rely on approved mechanisms to lawfully transfer personal information across borders, such as standard contractual clauses or other model clauses approved for use by applicable data protection authorities. We generally will use Standard Contractual Clauses ("SCCs"), approved by the European Commission, as a legal mechanism for data transfers outside the European Union (EU); the Addendum to the SCCs, approved by the United Kingdom's ("UK") Information Commission, for transfers outside of the UK; and the Standard Data Protection Contractual Clauses (the "SDPCC"), approved by the Commissioner of Data Protection for the Dubai International Financial Centre ('DIFC"), for transfers outside of the DIFC. These clauses are contractual commitments between companies transferring personal information, binding them to protect the privacy and security of the transferred personal information. Please contact us using the contact details provided under Section 12 (Contact Us), below, if you would like to request a copy of the relevant standard data transfer clauses.

Return to the top.

8. Information Security

We work to secure your personal information from being lost, accessed, used, modified, or disclosed by/to unauthorized persons. During transmission of personal information between you and our Site, we use Transport Layer Security (TLS) software to encrypt information you input. Only employees who need the information to perform a specific job are granted access to personal information. These employees are made aware of our security and privacy practices. As another security measure, the servers that we use to store personal information are kept in a secure, restricted access area.

Please note that despite our reasonable efforts, no security measure is ever perfect or impenetrable, so we cannot guarantee the security of your personal information. Consequently, you should take steps to protect against unauthorized access to your password, phone, and computer by, among other things, signing off after using a shared computer, choosing a robust password that nobody else knows or can easily guess and keeping your log-in and password private.

Return to the top.

9. Retention of Personal Information

We keep personal information for as long as is reasonably required for the purposes explained in this Statement. We also hold records, which may include personal information, to meet legal, regulatory, tax, accounting and/or internal data retention policy needs. For example, we are required to retain an accurate record of your dealings with us, so we can respond to any complaints or concerns you or others might raise later. We'll also retain files if we reasonably believe there is a prospect of litigation. The specific retention period for your personal information will depend on your relationship with us and the reasons we hold your personal information.

Return to the top.

10. Information Rights Specific to Your Region

Additional State-Specific Information for Individuals Who Reside in the United States

Scope of This Section

This section applies only to individuals who reside in the states of California, Colorado, Connecticut, Montana, Oregon, Texas, Utah, and Virginia (collectively, "U.S. Residents"). This Section provides U.S. Residents with information that is not provided elsewhere in this Statement and is required by the law of the state where they reside (collectively, "Applicable State Privacy Laws").

This section does not apply to:

- information publicly available from government records or made publicly available by you or with your permission
- deidentified or aggregated information;
- protected health information covered by the Health Insurance Portability and Accountability Act ("HIPAA") or the Health Information Technology for Economic and Clinical Health Act ("HITECH");
- personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act ("FCRA"), or the Gramm-Leach-Bliley Act ("GLBA")
- any other personal information or entities excluded from the scope of Applicable State Privacy Laws.

Your Privacy Rights

Subject to any applicable limitations and exceptions, U.S. Residents have the following rights under State Privacy Laws:

- **Right to Access/ to Know**: You have the right to information about whether we process your personal information, to have access to such information, and certain details about how we use it. If you are a resident of California, you have the right to information about whether we process your personal information, and our collection, use, and disclosure of categories of your personal information. In addition, in lieu of a right to access, you have the right to submit a verifiable request to know specific pieces of your personal information obtained from or about you.

- **Right to Delete**: Except for residents of California and Utah, you have the right to submit a verifiable request to delete personal information that Brown & Brown has collected from or about you. If you reside in California or Utah, you have the right to submit a verifiable request to delete personal information that Brown & Brown has collected from you.

- **Right to Correct**: You have the right to submit a verifiable request to correct inaccurate personal information that Brown & Brown has collected from or about you, taking into account the nature of the personal information and the purposes of processing the personal information.

- **Right to Data Portability:** Except for residents of California, you have the right to obtain from the Company, or to ask the Company to send to a third party, a copy of your personal information in electronic form that you provided to the Company.

- **Non-Discrimination**: Brown & Brown will not unlawfully discriminate against you for exercising your privacy rights under Applicable State Privacy Laws.

If you reside in Oregon: In addition to the rights described above, you also have the right to obtain, at Brown & Brown's option, a list of specific third parties to which we have disclosed either your personal information, or any personal information.

How to Exercise Your Privacy Rights

To exercise your rights, please submit a request to us by visiting our online privacy rights portal and completing the request ***webform***.

Alternatively, you may call us at **+1 (888) 914-9661** and enter the following **PIN: 363 845** when prompted to do so. You will be asked to provide information necessary for us to process your request.

Except for residents of California and Utah, U.S. Residents may also have the right to appeal any decision we make in response to a request to exercise privacy rights, by using the webform or by calling us at the telephone number listed above. We will inform you of any action taken in response to an appeal, along with a written explanation of the reasons for our decision(s), in accordance with Applicable State Privacy Laws.

How We Will Verify Your Request

If you submit a request, we match personal information that you provide us against personal information we maintain in our files. The more risk entailed by the request (e.g., a request for specific pieces of personal information), the more items of personal information we may request to verify your identity. If we cannot verify your identity to a sufficient level of certainty to respond securely to your request, we will let you know promptly and explain why we cannot verify your identity.

Authorized Agent

If an authorized agent submits a request to know, correct, or delete on your behalf, the authorized agent must submit with the request a document signed by you that authorizes the authorized agent to submit the request on your behalf. In addition, we may ask you to follow the applicable process described above for verifying your and the authorized agent's identity. You can obtain an "Authorized Agent Designation" form by contacting us at it@bbins.com.

Additional Information for California Residents

The California Consumer Privacy Act as amended by the California Privacy Rights Act (the "CCPA") requires the following additional information for California residents. The information below concerning the collection and disclosure of California residents' personal information as well as the information in Sections 3 through 6, above, apply to Brown & Brown's collection, use, and disclosure of California residents' personal information during the twelve months preceding the last updated date of this Privacy Statement and prospectively.

Notice at Collection

The Company collects the categories of personal information identified in Section 3 (Personal Information We Collect About You), above, for the purposes identified in Section 5 (How We Use Your Personal Information), above, and retains personal information for the period described in Section 9 (Retention of Personal Information), above. We do not, and will not, sell your personal information or disclose it to third parties for cross-context behavioral advertising ("sharing"). In addition, we have no actual knowledge that we sell or share the personal information of individuals of any age, including the personal information of children under 16. We also do not collect or process sensitive personal information for the purpose of inferring characteristics about you.

Additional Information About the Categories of Personal Information We Collect

The personal information we collect falls within the following "categories of personal information" listed in the CCPA:

- **Identifiers**, such as your name, telephone number, and email address.
- **Professional or Employment-Related Information**, such as your employer, job title, and other information necessary for the administration of the relationship between Brown & Brown and your employer.
- **Commercial Information**, such as records of services purchased, and purchasing or consuming histories.
- **Internet or other electronic network activity information**, including your interactions with the Site.

- **Sensory or Surveillance Data**, for example: voice-mails, recordings of telephone calls with our service center representatives, recordings captured by equipment at our offices and other physical locations.

- **Characteristics of Protected Classifications Under California or Federal Law**, such as your age, gender, or marital status, where relevant to the Service provided.

- **Personal information listed in the California Customer Records statute** (Cal. Civ. Code §1798.80(e)), to the extent not already included in other categories here, such as benefit elections, pension entitlement information, and certain medical records.

Additional Information About Disclosures of Personal Information

We may disclose your personal information to third parties for the following "business purposes" as that term is defined in the CCPA and as a supplement to the disclosure described in Section 6 (How We Disclose Personal Information), above:

- **Service providers:** We may disclose any of the categories of personal information listed above to service providers for the business purpose of performing services on the Company's behalf.

- **Professional Advisers and Related Third Parties:** We may disclose the categories of personal information listed above to the professional services providers listed in Section 6 (How We Disclose Personal Information), above, for the business purpose of auditing compliance with policies and applicable laws.

- **Affiliated companies:** We may disclose any of the categories of personal information listed above to other companies within the Brown & Brown family of companies for the business purposes of: (a) auditing compliance with policies and applicable laws, (b) helping to ensure security and integrity, (c) debugging, (d) short-term transient use, (e) internal research, and (f) activities to maintain or improve the quality or safety of a service or device.

Note on Deidentified Information

At times, Brown & Brown converts California residents' personal information into deidentified information using reasonable measures to ensure that the deidentified information cannot be associated with the individual ("Deidentified Information"). We maintain Deidentified Information in a deidentified form and do not attempt to reidentify it, except that we may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes ensure that the information cannot be associated with the individual. Brown & Brown prohibits vendors, by contract, from attempting to reidentify the Company's Deidentified Information.

Additional Information Specific to Individuals Who Reside Outside the United States

If you reside in Bermuda, Canada, the Dubai International Financial Center (DIFC), European Union ("EU"), Hong Kong, Malaysia, or the United Kingdom ("UK") (collectively, "Non-U.S. Residents"), the following also applies to you:

Your Rights With Respect to Your Personal Information

Subject to any limitations and exceptions provided by the law applicable to your country of residence, you have the right to:

- request **access** to your personal information, i.e., to ask the Company to provide you with copies of your personal information;

- request that the Company **update, correct or delete** (the "right to be forgotten") your personal information, i.e., to rectify personal information that is incomplete or inaccurate or to erase your personal information;

- **withdraw your consent** to the processing of your personal information, at any time, where you previously consented to the processing of your personal information. If the Company requests your consent to process your personal information and you do consent, you may use the contact information below to withdraw your consent. Any withdrawal shall not affect the lawfulness of processing based on your consent before its withdrawal, and the Company will continue to retain the information that you provided us before you withdrew your consent for as long as allowed or required by applicable law. In addition, if Brown & Brown has an alternative lawful ground for processing your personal information without your consent, the Company may continue processing your personal information based on that alternative lawful ground for processing.

- **lodge a complaint with the supervisory authority** where you live, where you work, or where you believe the violation occurred if you believe that your personal information has been processed in violation of applicable data protection law.

    - DIFC residents may contact the DIFC Commissioner of Data Protection here: https://www.difc.ae/.

    - EU residents can find contact information for your data protection authority here: https://edpb.europa.eu/about-edpb/board/members_en

    - UK residents can find contact information for your data protection authority here: https://ico.org.uk/.

    - Canada residents may contact the Office of the Privacy Commissioner of Canada here: https://www.priv.gc.ca

    - Bermuda residents may contact the Office of the Privacy Commissioner of Bermuda here: https://www.privacy.bm

    - Hong Kong residents may contact the Office of the Privacy Commissioner for Personal Data here: https://www.pcpd.org.hk

    - Malaysia residents may contact the Personal Data Protection Commissioner here: https://www.pdp.gov.my

Additional Rights Applicable to DIFC, EU, and UK Residents

Subject to any limitations and exceptions provided by the law applicable to your country of residence, DIFC, EU and UK residents also have the right to:

- request **restriction of processing** of your personal information in certain situations, such as while a dispute concerning the accuracy of personal information is being resolved;

- request **data portability**: Subject to certain limitations, the right to data portability allows you to obtain from the Company, or to ask the Company to send to a third party, a copy of your personal information in electronic form that you provided to the Company.

- **object to the processing** of your personal information: You have the right to object to the processing of your personal information based solely on the Company's legitimate interests. If you do object in these circumstances, the processing of your personal information will be stopped unless there is an overriding, compelling reason to continue the processing or the processing is necessary to establish, pursue or defend legal claims.

How to Exercise Your Privacy Rights

For DIFC, EU, UK, Hong Kong and Malaysia residents: you can exercise your rights by submitting a request to us at data.protection@bbrown.com or via mail to Brown & Brown, Europe 7th Floor, Corn Exchange, 55 Mark Lane, London EC3R 7NE, United Kingdom. The Company will respond to such requests in accordance with applicable data protection law.

For Canada and Bermuda residents: to exercise your rights, please submit a request to us by visiting our online privacy rights portal and completing the request ***webform***. Alternatively, you may call us at **+1 (888) 914-9661** and enter the following **PIN: 363 845** when prompted to do so. You will be asked to provide information necessary for us to process your request. The Company will respond to such requests in accordance with applicable data protection law.

Additional Information for Residents of Bermuda

If you reside in Bermuda: In addition to the rights described above, you also have the right to object to the processing of your personal information: (a) for purposes of direct marketing; or (b) where the processing causes or is likely to cause substantial damage or distress to you or others.

Additional Information for Individuals Whose Personal Information is Processed by Nexus Underwriting (DIFC), Ltd.

If Nexus Underwriting (DIFC), Ltd., processes your personal information, you may exercise the rights described above which apply to residents of the Dubai International Financial Centre.

Additional Information for Residents of Malaysia

If you reside in Malaysia: In addition to the rights described above, you also have the right to object to the processing of your personal information: (a) for purposes of direct marketing; or (b) where the processing causes or is likely to cause substantial damage or distress to you or others.

Return to the top.

11. Children

We do not knowingly collect personal information directly from children under the age of 13. Our Services are marketed towards adults who may provide us with personal information concerning their children under the age of 13 in connection with our services, for example, where a child under the age of 13 is named as a dependent or beneficiary on an insurance policy. If we are notified that we have collected the personal information of a child under the age of 13 directly from the child and without verifiable parental consent, we will delete the personal information from our files as expeditiously as possible.

Return to the top.

12. Contact Us

If you have any questions about this Statement or the rights conferred to you under the applicable data privacy law, please contact us at the **Brown & Brown's Global Privacy Office** at privacy@bbins.com or at the following addresses/emails/telephone numbers:

- **UK contact:** Brown & Brown, Europe 7th Floor, Corn Exchange, 55 Mark Lane, London EC3R 7NE, United Kingdom data.protection@bbrown.com.
- **US contact:** Brown & Brown, Inc. 300 N. Beach Street, Daytona Beach, Florida, 32114, United States privacy@bbins.com.
- **Bermuda Data Protection Officer**: If you reside in Bermuda and have questions concerning this Statement or regarding the handling of your personal information, you may contact Jennifer Masters, Privacy Officer for Beecher Carlson Insurance Services LLC., Beecher Carlson Bermuda, Maxwell Roberts Building, 1 Church Street, 7th Floor, P.O. Box 2461, Hamilton, HMJX Bermuda at jennifer.masters@bbrown.com or via telephone at 441-591-2501.
- **Canada contact:** If you reside in Canada and have questions concerning this Statement or regarding the handling of personal information, you may contact John Carlton, Customer Privacy Department, at jcarlton@bbrown.com.

Return to the top.

13. Changes to the Statement

We review this Statement regularly and may make changes at any time to take account of changes in our business activities, legal requirements, or the manner in which we process personal information. We will place updates on this website and where appropriate we will give reasonable notice of any changes. You should periodically review this Statement to ensure you understand how we collect and use your personal information.

Return to the top.