

Global Travel Safety Association Privacy Policy

Global Travel Safety Association and Keen Bond Asia Holding Ltd, hereinafter referred to as "GTSA," is committed to protecting the privacy and security of the personal information we collect while providing products and services to our customers. GTSA and the companies with which we work to provide coverages and services to our customers each perform distinct services that may not apply to your situation. This Global Privacy Policy is designed to encompass all of the services provided by our collaborating companies, so references to the sale of insurance policies, for example, may not apply to your specific situation. However, the aim of this Global Privacy Policy is to inform you about the ways in which we collect, process, and handle your personal information, as well as your rights and options.

Purposes for Processing

GTSA may process your personal data for one or more of the following purposes:

- Purchasing a travel, health, or other type of insurance policy
- Medical assistance
- Technical assistance
- Security assistance
- Administering and/or servicing insurance policies
- Handling a claim/working with an insurer to assess if a claim is covered by an insurance policy

Legal Basis for Processing

We rely on the following legal bases for managing your personal data:

- Consent
- Performance of a contract
- Vital interests

Recipients of Data

Personal information may be shared with companies affiliated with GTSA and non-affiliated third parties in the United States and other countries, to fulfill the purposes outlined above, and as otherwise permitted or required by law. The following categories of recipients may be involved:

- Insurers
- Assistance Companies or repatriation service providers
- Telehealth Services
- Translation Services
- Hospitals or other medical practitioners
- Other affiliated GTSA entities, contractors, and IT Service Providers

When we share personal data with third parties, we require those third parties (where applicable) to maintain a comparable level of protection of personal data as set out in this Privacy Notice. On request and where required by law,

we will confirm the name of each third party to which your personal data has, or will be, transferred. To the fullest extent permitted by applicable law, we disclaim all liability for the use of your personal data by third parties.

Categories of Personal Data Processed

For the purposes outlined above, GTSA may collect, process, and store the following categories of personal data:

- Identity Data: first name, surname, email address, home address, telephone number, mobile number, date of birth, gender, location, nationality, insurance details, government identification numbers such as U.S. Social Security number (SSN), Employer Identification Number (EIN), copy of passport, copy of driving license, next of kin if customer is incapacitated
- Medical Data: any information relating to existing medical conditions, current medical status, injuries sustained while travelling, medical diagnosis, provider name and contact information, details of assault
- Travel Data: flight details, policy issued start date and end date, car rental information, motorbike rental information
- Technical Data/Metadata: includes internet protocol (IP) address, unique mobile device identification numbers (such as your Media Access Control (MAC) address, and/or International Mobile Equipment Identity (IMEI), type of device, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our website

Transfer to a Third Country

GTSA may transfer your personal data to other countries, in the course of providing services to you. There is an agreement or agreements in place with the other entities of GTSA. When transferring your personal data, we will take reasonable measures to ensure that it is protected and that the transfer is lawful. In instances where data is transferred, we do so in accordance with our legal bases of fulfilling a contract, health and professional services and your explicit consent.

Retention of Data

GTSA may retain personal data of customers for a period of up to seven (7) years, after which time it is destroyed/erased from our records.

Data Received from a Third Party

Personal information may be received from such sources as our affiliates, insurers, independent insurance brokers, other financial institutions, credit bureaus, government departments, claims organizations, a policyholder, a customer, a customer's employee, a claimant, a claimant's employer, or a claimant's employee.

Your health information, such as pre-existing medical conditions, is generally required to arrange travel insurance, to make a determination on a claim or to provide you with medical assistance. If you make a telephone call into one of our service centers, the call may be recorded for training and quality control purposes. You will be informed if your call is being recorded.

If you provide health information to your agent or consultant to provide to us as part of the policy application or claims process, we rely on you having provided them with your consent to disclose this information to us. In addition, when you provide information, including sensitive information about other individuals on your travel insurance policy, we rely on you to inform them of the information you are providing, how we will use, hold, collect and disclose this information and on you obtaining their consent.

Technical and Organizational Measures

To secure your personal data, GTSA has implemented appropriate technical and organizational measures. Access to personal information is limited to those with a specific “need to know” to provide products and services to policyholders and to others as permitted or required by law. We maintain where practical, contractual, physical, electronic, and procedural safeguards to protect against the misuse of personal information under our control.

Data Subject Rights

As a customer of GTSA, you have the following rights which you can exercise with GTSA at any time.

- Right of Access

You have the right to access your personal information kept on file by us. To exercise this right, please send a request in writing to our Privacy Officer at the address provided below. Please specify the kind of information you are seeking. You will be contacted by our Privacy Officer and asked to provide some form of identification to confirm your right to access this information.

- Right of Rectification

You have the right to correct any personal information that we hold about you, subject to our verification.

- Right to Erasure

You have the right to request the deletion of the personal data that we hold about you.

- Right to Restriction of Processing

You have a right to request that processing of personal data is restricted in certain circumstances. However, we reserve the right to continue to process the personal data for storage purposes, for the establishment, exercise, or defense of legal claims or with your consent.

- Right to be Notified

You have the right to be informed about the uses of your personal data in a clear manner and be told the actions that can be taken if you feel your rights are being impeded. You also have the right to be informed of any rectification or erasure of your personal data.

- Right to Data Portability

You have the right to request that your personal data file is sent electronically to a third party. This data will be provided in a commonly used, machine readable format, if doing so is technically feasible.

- Right to Object

Where we are relying on legitimate interests as a legal basis to process your data, you have a right to object to such processing on grounds relating to your situation.

Rights of Customers are not absolute. While you may have some, or all, of the rights enumerated above, in certain situations those rights cannot be granted. For example, but not limited to, the right to restrict data processing does not apply when data is processed for the purposes of the prevention, investigation, detection, or prosecution of criminal offenses. The same applies to the processing of personal data in the prevention of threats to public security.

You have the right to access your personal data file, although not if that access adversely affects the rights and freedoms of others. As applicable, personal information provided by you will be held and used in accordance with the terms of our privacy policy.

Children's Privacy

GTSA is concerned about children's privacy. This section of our privacy policy explains our information practices in connection with information provided by all children under the age of 18 whose parent or guardian's consent we require for certain uses of their information ("Child" or "Children").

We support the Children's Online Privacy Protection Act ("COPPA"). Our goal is to minimize the information gathered from and disseminated about Children while allowing us to provide the Services for which they are covered under policies of insurance.

Collection of Childrens' Data

We require parental/guardian consent to collect personal information about Children for the purposes of providing the Services. Children's personal information is used for the same purposes as set out above.

How is Personal Information About Children Used?

We use personal information to administer or service a policy; administer a claim; provide assistance and security services; comply with the law; and as otherwise permitted by law. The transfer of Children's personal information to an affiliate or third party for processing purposes is defined as a "use" of your personal information.

GTSA uses the personal information of Children solely for the purposes for which that consent was required. All other sections of this Privacy Policy apply to the personal information of Children.

Additional Information if you are resident in California or Nevada

What Are My Privacy Rights as a California Resident?

If you are a California resident, California law may provide you with additional rights regarding our use of your personal information; subject to exclusions from the rights granted under California law with respect to certain information governed by certain sector-specific privacy laws.

Subject to certain exceptions under California law, California residents may have the following rights with respect to their personal information collected by GTSA:

The right to know and access. California residents have the right to request we disclose (i) a copy of the personal information that we collect about you; (ii) the categories of personal information that we collected about you in the preceding 12 months; (iii) the categories of purposes for which such personal information was disclosed in the preceding 12 months; (iv) the categories of sources such personal information was collected for; and (v) the categories of third parties such personal information may have been shared with.

The right to deletion. California residents have the right to request that we delete the personal information that we or our vendors collected about you. There may be circumstances under which we will be unable to delete your personal information, such as if we need to comply with our legal obligations or complete a transaction for which your personal information was collected. If we are unable to comply with your request for deletion, we will let you know the reason why.

The right to equal service. If a California resident chooses to exercise any of these rights, we will not discriminate against the California resident in anyway. However, if a California resident exercises certain rights, such California resident may be unable to use or access certain features of the Sites.

Exercising California Resident Rights

To exercise any of these rights, please contact our Privacy Officer using the contact details below. In connection with submitting a request, you must provide the following information: name, email, phone number, state of residence, and policy number and you must state what type of request you are making.

We have the right to require you to provide written permission granting authority to your representative and for your agent to verify its identity directly with us, and we may deny a request from your representative who does not submit proof of authorization as we request.

A California resident may only make a verifiable consumer request for access or data portability twice within a 12-month period. The request must provide sufficient information that allows us to reasonably verify the requestor is the person about whom we collected personal information or an authorized representative and describe the request with sufficient detail that allows us to properly understand, evaluate, and respond to it. We cannot respond to a request or provide personal information if we cannot verify the identity or authority to make the request.

We will endeavor to confirm receipt of a request within 10 working days following submission and provide information about how we will process the request. We will endeavor to respond to a verifiable consumer request within 45 days of its receipt. If we require more time (up to an additional 45 days), we will provide notice in writing explaining the reason for the extended time period. We may deliver our written response by mail or electronically, at your option.

Any disclosures we provide will only cover the 12-month period preceding the request receipt date. If we deny a request, we will provide a response explaining the reasons we cannot comply with a request, if applicable.

Sharing of California Resident Personal Information

We may have collected and disclosed the following categories of personal information from a California resident for a business purpose in the preceding 12 months:

- Various identifiers, including, name, address, online identifier, Internet Protocol (IP) address, email address, account name, or other similar identifiers.
- Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)), including, telephone number or financial information.
- Geolocation data, including, physical location or movements. Protected classification characteristics, including, race, color, national origin, marital status, sex, veteran, or military status.
- Personal records, such as, power of attorney, family history or power of attorney.
- Information received from a government entity or other third party.

We may collect the above categories of personal information directly from you, indirectly as you interact with our website, from or through other third-party sources, including our customers, or through email or other electronic messages between you and our website.

In the prior 12 months, we may have disclosed the categories of personal information set forth above for one or more of the purposes set forth in this privacy policy. We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Sale of California Resident Personal Information

In the prior 12 months, we have not sold personal information of a California resident.

“Shine the Light” Law

California’s “Shine the Light” law, Civil Code section 1798.83, requires certain businesses to respond to requests from California consumers asking about the business’ practices related to disclosing personal information to third parties for the third parties’ direct marketing purposes. To make such a request, please contact our Privacy Officer using the contact details below.

How We Respond to “Do Not Track” Signals

Our website does not respond to DO NOT Track signals. Third parties cannot collect any other personally identifiable information from our website unless you provide it to them directly.

What Are My Privacy Rights as a Nevada Resident?

Nevada residents may have certain rights to opt-out of sales of their personal information under Nevada Revised Statutes Chapter 603A. However, please know GTSA does not sell data triggering this Nevada statute’s opt-out requirements. If you have questions with respect to this right, please contact our Privacy Officer using the contact details below.

Your privacy on the internet and when using mobile devices What Are My Choices?

Location Information: With your consent, we may collect information about your actual location when you use our mobile applications and when you request or purchase products or services. You may stop the collection of this information at any time by changing the settings on your mobile device; but note that some features of our mobile applications may no longer function if you do so.

Native Applications on Mobile Device: Some features of our mobile applications may require access to certain native applications on your mobile device, such as the camera, photo album and the address book applications. If you decide to use these features, we will ask you for your consent prior to accessing the applications and collecting associated information. Note that you can revoke your consent at any time by changing the settings on your device.

Cookies: Most web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove or reject browser cookies. Please note that if you choose to remove or reject cookies, this could affect the availability and functionality of the website.

Push Notifications: With your consent, we may send push notifications or alerts to your mobile device. You can deactivate these messages at any time by changing the notification settings on your mobile device or within our mobile applications.

Other state privacy regulations

As other U.S. states develop privacy regulations that affect GTSA customers, we reserve the right to implement policies and practices to comply with those regulations.

GTSA HIPAA Policy

Global Travel Safety Association “GTSA” is committed to protecting the privacy and security of individually identifiable health information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and its regulations. This policy outlines the procedures and safeguards implemented by GTSA to ensure the confidentiality, integrity, and availability of protected health information (PHI) in the course of our travel risk management insurance and assistance program operations.

Scope:

This policy applies to all employees, contractors, and business associates of GTSA who have access to PHI while providing travel risk management insurance and assistance services.

Key Responsibilities:

1. Privacy Officer: GTSA designates a Privacy Officer responsible for overseeing HIPAA compliance, conducting regular risk assessments, and ensuring that policies and procedures are implemented and followed.
2. Training and Awareness: All employees and relevant stakeholders receive HIPAA training upon onboarding and annually thereafter. This training covers the importance of PHI confidentiality, proper handling of PHI, and reporting procedures for potential breaches.
3. Use and Disclosure of PHI:
 - a. PHI is only accessed by authorized individuals for legitimate business purposes.
 - b. PHI is not disclosed to unauthorized parties without explicit consent or as permitted by law.
4. Physical and Technical Safeguards:
 - a. Physical access to areas containing PHI is restricted.
 - b. Electronic systems containing PHI are secured as practical with access controls.
5. Incident Reporting and Response:
 - a. Any suspected or actual breaches of PHI must be reported to the Privacy Officer immediately.
 - b. GTSA has an incident response plan in place to address and mitigate breaches promptly.
6. Business Associate Agreements:
 - a. Business associates handling PHI on behalf of GTSA are required to have HIPAA-compliant business associate agreements.

Documentation and Recordkeeping:

All HIPAA-related policies, training records, risk assessments, and incident reports are documented and retained in accordance with HIPAA regulations.

Policy Review and Updates:

This HIPAA policy is regularly reviewed and updated to reflect changes in regulations, business processes, or technology that may impact the security of PHI.

Enforcement:

Violations of this HIPAA policy by GTSA associates or affiliated third parties may result in disciplinary action, including termination, as well as legal consequences.

Effective Date:

This HIPAA policy is effective as of January 1, 2024 and will be reviewed annually for continued relevance and compliance.

What if I have a question, concern, incident report, or complaint?

Please contact our Privacy Officer using the information provided below.

GTSA Privacy Officer
Privacy@Globaltravelsafetyassociation.com

This privacy policy is a stand-alone document. You may receive privacy policies, statements, or notices from other parties. The terms of this privacy policy do not modify, supersede, revise, or amend the terms of other privacy policies, statements or notices received from other parties. We may update this privacy policy from time to time.