

## Blue Trust California Privacy Policy

**Effective Date:** January 1, 2020

**Last Updated:** July 25, 2024

This Blue Trust, Inc. (“Blue Trust”) California Privacy Policy (“California Policy”) applies solely to online visitors and users and other individuals who reside in the State of California and provide “personal information” (as defined below) to Blue Trust (“consumers” or “you”). This California Policy does not address personal information collected for workforce-related inquiries or transactions.

Any phone numbers collected by Blue Trust for SMS consent will not be shared, sold, or disclosed with third parties or affiliates for any purposes.

**If you are a prospective, existing or past Blue Trust customer residing in California and have been provided with a copy of our [Privacy Notice](#) at any time, any personal information collected as part of that client relationship will be used in accordance with our [Privacy Notice](#) and will not fall under this California Policy.**

We adopt this California Policy to comply with the California Consumer Privacy Act of 2018 (CCPA) and any terms defined in the CCPA have the same meaning when used in this policy.

### Information We Collect

Blue Trust collects information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device (“**personal information**”). In particular, Blue Trust has collected the following categories of personal information from its consumers within the last twelve (12) months:

1. **Identifiers**, such as real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver’s license number, passport number or other similar identifiers.
2. **Personal information categories listed in the California Consumer Records statute (Cal. Civ. Code § 798.80(e))**, such as name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. (Some personal information included in this category may overlap with other categories.)
3. **Protected classification characteristics under California or federal law**, such as age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).
4. **Commercial information**, such as records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies.
5. **Internet or other similar network activity**, such as browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.
6. **Geolocation data**, such as IP addresses, which are registered to a geographic location.
7. **Audio, electronic, visual, thermal, or olfactory information**, such as videos, photos, or voice recordings.
8. **Professional or employment-related information**, such as current or past job history.
9. **Other categories of personal information**, such as is described in the Blue Trust [Internet Privacy Policy](#).
10. **Inferences drawn from your personal information**, as identified above, to create a profile about you reflecting your preferences, trends, or behaviors.

Personal information does not include:

- Publicly available information from government records.

- Deidentified or aggregated consumer information.
- Information excluded from the CCPA's scope, including:
  - health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data;
  - personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

Blue Trust obtains the categories of personal information listed above from the following categories of sources:

- **Directly from you or your agents.** For example, from documents you complete or information you tell us.
- **Indirectly from you.** For example, from website usage details collected automatically on our website.
- **From our affiliate companies.**
- **From third parties.** For example, from individuals who provide information about you in connection with our provision of services to a trust, estate, guardianship or other fiduciary relationship for which you are a beneficiary or other related party.

#### **Use of Personal Information**

We may use or disclose the personal information we collect for one or more of the following purposes:

- To fulfill or meet the reason you provided the information. For example, if you share your name and contact information to ask a question about our services, we will use that personal information to respond to your inquiry. As another example, if you provide personal information in connection with a trust which we administer, we will use that information to administer the trust.
- To provide, support, personalize, and develop our website and services.
- To create, maintain, customize, and secure accounts with us for business or fiduciary entities you represent.
- To process your requests or transactions and prevent transactional fraud.
- To provide you with support and to respond to your inquiries, including to investigate and address your concerns and monitor and improve our responses.
- To help maintain the safety, security, and integrity of our website, services, databases and other technology assets, and our business.
- For testing, research, and analysis, including to develop and improve our website and services.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- As described to you when collecting your personal information or as otherwise set forth in the CCPA.
- To learn about opportunities to market other services that may be of interest to you and to market those services to you.
- To conduct internal research, such as to measure consumer interaction with Blue Trust online.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Blue Trust's assets, whether as a going concern or as part of receivership, liquidation, or similar proceeding, in which personal information held by Blue Trust about our consumers is among the assets transferred.

Blue Trust 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.

### **Sharing Personal Information**

Blue Trust may disclose the information we collect about you, as listed above, with other parties. Specifically, we share personal information with the following categories of other parties:

- **Service providers:** We may share all categories of information we collect with service providers who perform services on our behalf for business purposes, including marketing. When we disclose personal information to service providers, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract.
- **Government agencies and regulators:** We may share all categories of information we collect with government agencies and regulators for business purposes to demonstrate our compliance with, or as required by, various laws and regulations.
- **Third parties:** With your consent, we may share internet or other similar network activity we collect with third parties to perform targeted marketing. We may also share information with third parties if required by law to do so.

### **Sale of Personal Information**

Blue Trust does not sell the personal information of any California consumers.

### **Minors Under 16**

Blue Trust does not knowingly sell the personal information of minors under 16 years of age without affirmative authorization.

### **Your Rights and Choices**

If you are a California consumer, you have specific rights under California law regarding your personal information (unless you are a prospective, current or former customer of Blue Trust, in which case your rights are described in our [Privacy Notice](#)). This section describes the rights applicable to California consumers and explains how to exercise them.

#### ***Access to Specific Information and Data Portability Rights***

You have the right to request that Blue Trust disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request (see Exercising Access, Data Portability, and Deletion 0), we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting that personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you (also called a data portability request).
- If we disclosed your personal information for a business purpose, the personal information categories that each category of recipient obtained.

#### ***Deletion Request Rights***

You have the right to request that Blue Trust delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request (see Exercising Access, Data Portability, and Deletion 0), we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

1. Complete the transaction for which we collected the personal information, provide a service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.

2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Debug to identify and repair errors that impair existing intended functionality of our services.
4. Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
5. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 *et. seq.*).
6. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.
7. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
8. Comply with a legal obligation.
9. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

### ***Exercising Access, Data Portability, and Deletion Rights***

To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request to us by either:

- Calling us at (833) 342-0984; or
- Submitting this online [form](#).

Only you, or someone legally authorized to act on your behalf (an “Authorized Agent”), may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child. We may request written permission from you before honoring any requests made by an Authorized Agent. Any identity verification, noted below, may still need to be completed by the consumer directly.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative. If there is a need to verify your identity prior to releasing information in accordance with your request, we will contact you at the phone number you provided in your request submission. At that time, we will conduct additional knowledge-based authentication to ensure that only those people who have a legal right to obtain information can do so.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you. Making a verifiable consumer request does not require you to create an account with us. We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

### ***Response Timing and Format***

We endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option.

Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

### **Non-Discrimination**

We will not discriminate against you for exercising any of your CCPA rights.

#### **Changes to This California Policy**

Blue Trust reserves the right to amend this California Policy at our discretion and at any time. When we make changes to this California Policy, we will post the updated California Policy on our website and update the policy's effective date.

#### **Contact Information**

If you have any questions or comments about this California Policy, the ways in which Blue Trust collects and uses your information described below and in our [Internet Privacy Policy](#) or [Privacy Notice](#), your choices and rights regarding such use, or wish to exercise your rights under California law, please do not hesitate to contact us at:

**Email:** [BlueTrustCompliance@bluetrust.com](mailto:BlueTrustCompliance@bluetrust.com)

**Phone:** (833) 342-0984

**Postal Address:**

Blue Trust

Attn: Compliance Department

1125 Sanctuary Parkway, Suite 500

Alpharetta, GA 30009