

# Privacy Policy

1. Introduction. At AstraVPN, we believe it's important that everyone, regardless of their situation, can obtain secure and private access to the internet. We always aim to provide this access without compromising the privacy of our customers. AstraVPN is provided by CODETRA LIMITED, (hereinafter referred to as "we", "us", or "our").

This Privacy Policy describes our privacy practices across the various products, services, applications, and websites that link to this policy (we refer to these collectively as our "Services", or individually as a "Product" or "Service"). This Privacy Policy applies to the access or use of our Services, and you agree to be bound by this Privacy Policy if you access or use our Services. If you do not agree with this Privacy Policy or any provisions hereof, please do not use our Services.

Though many of our Services are made available to consumers directly, some of our Services are offered to businesses or enterprise customers. For those Services, our customer is a business entity or other organization that may authorize individual end users (e.g. employees or customers) to use the Services that it has purchased or licensed from us. Where an organization is our customer, it may maintain accounts with us through which it and its users may submit information ("Customer Data"). In such cases, the organization that purchased or licensed our Services typically controls those accounts associated with their users and the organization may receive some Customer Data in order to maintain the account. In this case, we are generally a processor of Customer Data and the organization is the controller of such Customer Data. See the 'Disclosure of Information' section below for additional details.

To contact us, please see the "Contact Us" section below for more information.

2. What Information Do We Collect About You? This section describes the categories of personal data (or 'personal information') we may collect from and/or about you. The types of information described below are not collected in all situations and may vary depending on the Service you use. We collect the applicable information you provide through your use of a Service or Services, or as needed in specific Service-specific situations. For example, our VPN Products only collect a limited amount of personal data, and specifies that the collection of any websites or apps visited during a VPN session are not connected to any individual user, and therefore cannot be used for advertising or marketing purposes.

2.1. Information You Provide to Us

- Account Information. If a Service requires, or allows you to create, an account before you can access the Service, then we may collect information such as your name, username, email address, and password as a part of the account registration process.
- Billing and Payment Information. In order to purchase a Service, you may need to provide us and/or our payment processing partners with personal information such as your billing name, billing contact details (such as street addresses and/or email addresses), and payment instrument details. This basic billing information is used for payment processing and refund requests.
- Communications and Submissions. You may choose to provide us with information when you communicate with us (e.g. via email, phone, or chat for support or to inquire about our Services), including when you fill out an online form, respond to surveys, provide feedback, post comments to our website, participate in promotions, or submit information through our Services.

## 2.2 Information Collected when You use Our Services.

- Usage information. We collect information about how you interact with our Services, including when you visit and use our websites or apps, and when and for how long you use our Services. We may use cookies and/or other technologies to collect this information. See Section 6 for more information on how we use cookies and other technologies.
- Device information. We collect information from and about the device you use to access our Services, including information about the browsers and apps you use to access our Services. For example, we may collect device or mobile advertising identifiers, browser types, device types and settings, operating system versions, mobile, wireless, and other network information (such as internet service provider name, carrier name and signal strength), and application version numbers. We may use cookies and other technologies to collect this information See Section 6 for more information on how we use cookies and other technologies.
- Diagnostic information. We may collect information about the nature of the requests that you make to our servers, such as what is being requested, information about the device and app used to make the request, timestamps, and referring URLs.
- Approximate location information. Unless otherwise expressly stated or with your consent, we do not collect your location information based on your device's GPS or other device sensor data. However, we may collect your approximate location by calculating an imprecise latitude and longitude based on your IP address to provide you with better service (e.g. to connect you to the nearest and fastest VPN server).
- VPN Service Specific Information. Our VPN Products do not log any information that associates your account credentials or identity with your VPN session activity.

We do not maintain any records that show what websites you were browsing or apps accessed through a VPN connection. However, we will:

- Identify the locations of the VPN servers utilized
- Collect similar diagnostic information as referenced above.
- Ask you to rate your connection and provide some more detailed survey information if you are not satisfied with the service. Note this information is not tied to a specific user.
- We may also assign your device a 'hash', which is a random ID generated when you first launch one of our VPN apps. Device hashes are not linked to VPN browsing activity or user identity, but may be used to measure individual user activity.

### 2.3. Information Provided to Us by Third Parties.

- Third Party Invitation. If you are invited to use one of our Services, the party who invited you may submit your personal data or contact information, such as your email address, to us.
- Third Party Accounts. Some Services may allow you to register an account using a third-party account (such as a Google or Microsoft account) you have. If you elect to register or enroll in our Services through your third-party account, that third party may send us information about you that they have, such as email address or account identifying information that will enable us to provide our Services to you. What information is shared with us is controlled by the applicable third party that you have an account with. You may be able to control what information they send us via your privacy settings for that third party account.
- Threat Information. We receive information from reputable members of the security industry who provide information to help us to provide, develop, test, and improve our Services (for example, lists of malicious URLs, spam blacklists, phone number blacklists, and sample malware). Some of this information provided by third parties may contain personal data such as name or IP address on an incidental basis.

3. How Do We Use Your Information? We use the information we collect for various purposes described in this section. For visitors from the European Economic Area (EEA) or U.K., we also describe, below, our lawful basis for processing personal data.

- To provide, maintain, troubleshoot, and support our Services. We use your information for this purpose on the basis that it is required to fulfill our contractual obligations to you. Examples include:
  - For our VPN Product, using information about how much bandwidth you use and how long you use our Services in order to provide the Services in accordance with a plan to which you have subscribed;

- For our digital threat platform, using threat and device information to determine whether certain items pose a potential security threat; and
- Generally, to ensure the proper functioning of our Services.
- For billing and payment purposes. We use your information in order to perform billing administration activities and process payments, which are required to fulfill our contractual obligations.
- To communicate with users and prospective users. We use your information to communicate with you, including by responding to your requests, and sending you information and updates about our Services. We may do this in order to fulfill our contract with you, because you consented to the communication, or because we have a legitimate interest in providing you with information about our Services.
- To improve our Services. We want to offer you the best Services and user experiences we can, so we have a legitimate interest in continually improving and optimizing our Services. To do so, we use your information to understand how users interact with our Services. For example, we (a) analyze certain usage, device, and diagnostic information to understand aggregated usage trends and user engagement with our Services (and, for example, invest in technical infrastructure to better serve regions with increasing user demand); (b) may use device and threat information to conduct spam, threat, and other scientific research to improve our threat detection capabilities; and (c) review customer feedback to understand how we can improve.
- To develop new Services. We have a legitimate interest in using your information to plan for and develop new Services. For example, we may use customer feedback to understand what new Services users may want.
- To market and advertise our Services. We may use your information to provide, measure, personalize, and enhance our advertising and marketing based on our legitimate interest in offering you Services that may be of interest. For example, we may use information such as who or what referred you to our Services to understand how effective our advertising is; or we may use information to administer promotional activities such as sweepstakes and referral programs. Note that our VPN Products do not use your VPN browsing activity for these purposes and we do not maintain any records that show what you were browsing or accessing through a VPN connection.
- To implement security measures and prevent against harm or liability. We may use information for security purposes (such as to investigate security issues or to monitor and prevent fraud) and to prevent abuse. We may do this to comply with our legal obligations, to protect an individual's vital interests, or because we have a legitimate interest in preventing harm or liability to us and our users. For example, we may use account, usage, and device information to determine if an entity is engaging in abusive or unauthorized activity in connection with our Services.

- For compliance with legal obligations. We may use your information as required to comply with applicable law or regulation, legal process, or other legal obligation to which we are subject. For example, we may be compelled by a contract or court to provide certain information necessary to our business partners in order to fulfill the terms of a business agreement or our legal obligations. We may also use your information to enforce our legal rights and resolve disputes. To learn more about our practices regarding sharing your information with third parties for legal compliance purposes, see Section 4 below.

#### 4. Disclosure of Information - Who Do We Share Your Information With and Why?

We may disclose or use your information in the following circumstances, as applicable:

- In accordance with your instructions or consent. For example, some Services may allow you to register an account using a third-party account (such as a Google, Apple or Microsoft account). If you choose to do so, we will share information with the applicable third-party account provider you used.
- For collaborating with others on your behalf. Some Services may provide ways for different users to interact or collaborate with each other. Your information will be shared in connection with those activities if you choose to engage in them.
- To our vendors and service providers. Certain aspects of our Services are enabled or provided by third parties service providers and partners (including our affiliates) we engage, and we may disclose information to such companies and/or individuals we engage to perform business functions and services on our behalf. Such functions may include, for example:
  - processing of payments
  - providing analytics about our Services
  - providing sales and customer support
  - providing certain features or functionalities of our Services
  - maintaining or hosting the infrastructure required to provide our Services
  - delivering our marketing and advertising content.

Where your personal data may be shared with such third parties, we protect your data by entering into agreements containing appropriate confidentiality and data processing terms with the applicable third parties, reviewing their security practices, and limiting information sharing to the scope of what they are helping us with.

- To our corporate affiliates. We may disclose certain data or information to our affiliate entities for legitimate purposes, such as to provide certain Services that may be licensed by one of our affiliates to you.

- To a new owner(s) of our Services or any of our assets. If ownership or control of all or part of our Services, assets, or business changes, we may transfer your information to the new owner.
- For collection of aggregated or de-identified data. We may collect, use and share technical usage data or other user data that is aggregated and/or de-identified such that it no longer reveals the identity of an individual user for regulatory compliance, research and analysis, our own marketing and advertising activities, improvement of our Services, and other legitimate business purposes.
- To comply with legal processes and the law. We may share your information if we are required to do so by applicable law; to comply with our legal obligations; to comply with legal process; and to respond to valid law enforcement requests relating to a criminal investigation or alleged or suspected illegal activity that may expose us (or affiliates), you, or any of our other users to legal liability. If we share your information for these purposes, we limit the information shared to what is legally necessary, and challenge information requests that we believe are unlawful, overbroad, or otherwise invalid. To reiterate, our VPN Products do not collect information about which websites you visit or apps you use, so this information is not accessible in a law enforcement request.
- To enforce our rights and prevent fraud and abuse. We may share limited amounts of your information to enforce and administer our agreements with customers and users, and to respond to claims asserted against us or our affiliates. We may also share your information in order to protect against fraud and/or abuse against us, our affiliates, users and others.

6. Cookies and Other Tracking Technologies. We use various technologies in our Services to help us collect certain website or app user information.

These technologies include:

- Cookies. “Cookies” are small text files that can be placed on your computer or mobile device in order to identify your web browser and the activities of your computer on the Website. Cookies enable us or third parties that we allow (such as certain of our authorized service providers) to set cookies on your device to recognize visitors to our websites. For more information on how we use cookies, see section 6.1 below.
- Pixel Tags / Page Tags / Web Beacons / Tracking Links. These tools allow us to determine if you perform a specific action on a web page or email message. When you access a page, ad, or email, or click a link, these items let us know that you have accessed that page, opened an email, or clicked a link. They may also indicate your Internet Protocol (IP) address, which enables us to determine your approximate geographic location as assigned by your Internet Service Provider.

- Software Development Kits (SDKs) / Software. This mobile app software is provided by our business partners that enables our mobile apps to interact with the services those partners provide.

#### 6.1 Use of Cookies; Your Choices

- In general, we may use cookies in the following ways:
  - To provide our Services. Some cookies are essential for the proper operation of our Services. For example, cookies allow us to authenticate who you are and whether you're authorized to access a resource.
  - To store your preferences. Cookies can store your preferences, such as language preferences or whether to pre-fill your username on sign in forms. We may also use them to optimize the content that we show to you.
  - For analytics. Cookies are used to inform us how users interact with our Services so we can, as a legitimate interest, improve how they work (such as what screens or webpages you access, and whether our advertising is effective).
  - For security. Cookies can enable us and our payment processors to detect certain kinds of fraud.
  - For CODETRA LIMITED's advertising-related purposes. We advertise our Services online with the help of third parties who show ads and marketing about us on sites around the internet.
- Your Choices With Our Use of Cookies:
  - In general - You have the ability to manage your cookie preferences in your web browser settings, including deleting cookies and blocking cookies from being set on those browsers or devices. Visit the "help" section of your browser to understand what controls it gives you over cookies. Note that deleting or blocking certain cookies could adversely impact the proper operation of our Services, and, in some cases, some features of the website(s) may not function as a result.
  - Industry Advertising Choices - For information on how to opt out of personalized or interest-based advertising, you can visit the following pages:
    - U.S.: [Digital Advertising Alliance opt out page](#)
    - EU or UK: [Your Online Choices](#)

7. Information Security. We understand the importance of protecting information provided to or collected by us, including personal data, and employ reasonable and

appropriate methods (including a range of administrative, organizational, technical, and physical safeguards designed to protect your data such as use of best practices, procedures, policies, training, technology, and oversight) to protect against and reduce the risk of unauthorized access, loss, or release of data. Access to your account or services information is restricted to our employees or contractors who require such access to perform their job functions. While our controls are strong and we strive to protect your personal information through these various means, we cannot guarantee or warrant the security of the information, as no data security measures can guarantee 100% protection. We recommend you take every precaution in protecting your personal information when you are on the Internet or otherwise. You should change your passwords often, use a combination of letters and numbers when creating passwords, and make sure you use a secure browser.

8. International Data Transfers. Depending on where you reside and what Services you use, CODETRA LIMITED may transfer your personal data to countries other than the one in which you reside. We do this to facilitate our operations, and transferees include other CODETRA LIMITED companies, service providers, and partners. Laws in other countries may be different to those that apply where you reside. For example, personal data collected within the U.K., Switzerland or the European Economic Area (EEA) may be transferred and processed in the United States for purposes described in this policy. However, we put in place appropriate safeguards that help to ensure that such data receives an adequate level of protection, which typically includes CODETRA LIMITED and corporate recipients executing the Standard Contractual Clauses (aka 'Model Contracts') adopted by the European Commission or UK for such transfers to the U.S.

If you change your country of residence, the CODETRA LIMITED responsible for your data may change accordingly, and your data may be transferred to that other company.

For users of our VPN products, if you are a UK or EEA resident and you choose to use our software to route your Internet traffic through servers in countries not deemed 'adequate' by the UK or EEA, then you acknowledge that such transfers are executed at your direction and with your unambiguous consent.

9. Data Retention. We generally retain your personal information for as long as is needed to provide the Services to you, or for as long as you have an account or subscription with us. We retain your personal information as reasonably necessary for the respective purpose. In determining the criteria by which to retain or dispose of your information, we consider the type, sensitivity, context, and purpose of collecting the information. We may also retain personal information if required by law, or for our legitimate interests, such as abuse detection and prevention, and defending ourselves from legal claims. Residual

copies of personal data may be stored in backup systems for a limited period as a security measure to protect against data loss.

With respect to our VPN Products, we do not collect or retain data about your browsing activity while you are connected to the VPN Services.

10. Your Rights. Depending on your state or country of residence, you may have certain legal rights with respect to your personal information, subject to exceptions and limitations provided by applicable laws and regulations.

10.1 General. In general, you may have the following rights to your personal data:

- access and receive a copy of your personal data;
- correct your personal data;
- restrict the processing of your personal data;
- object at any time to the processing of your personal data;
- have your personal data erased;
- data portability;
- withdraw any consent you previously gave to the processing of your data (such as opting out to marketing communications);
- lodge a complaint with a data protection authority;
- request that we provide you with the categories of personal data we collect, disclose or sell about you; the categories of sources of such information; the business or commercial purpose for collecting or selling your personal data; and the categories of third parties with whom we share personal data. Note some of this information may already be provided in this Privacy Policy.

For clarity, the above describes examples of rights an individual may have. You may have some, but not all of the rights described above, depending on where you reside and what laws and regulations apply to you. Additional U.S. state specific privacy rights are further described below.

You may be able to exercise some of these rights by using the settings and tools provided in our Services. For example, you may be able to update your user account details via the relevant account settings screen of our apps. You may also be able to opt out from receiving marketing communications from us by clicking an “opt out” or “unsubscribe” link in such communications.

Some mobile and web browsers transmit "do-not-track" or "opt-out preference" signals. We currently do not take action in response to these signals. Otherwise, if you wish to exercise any of these rights, you may contact us using the details in the "Contact Us" section below. As permitted by law, we may ask you to verify your identity before taking further action on your request. You may also be permitted to designate an authorized agent to submit certain requests on your behalf. If you do so, you must give the authorized agent written permission to make such requests, or a power of attorney. We may also follow up with you to verify your identity before processing the authorized agent's request.

**10.2 Your California Privacy Rights.** The information provided in this Privacy Policy describes the categories of personal information We may collect, process and share with certain service providers and other businesses. If you are a California resident and would like to exercise your rights to receive the specific pieces of information, or other privacy rights applicable to you, please contact us as specified in the 'Contact Us' section below.

We do not 'sell' personal information for our own monetary benefit. However, as the CCPA defines 'sell' broadly, some of the advertising services that support our website, marketing efforts, and mobile applications use third party advertising services that may be deemed a 'sale' under California law. Please see Our terms relating to your choices relating to cookies and the app-specific advertising services listed above to indicate your preferences with respect to ads or cookie usage as applicable.

California residents also have the right to limit the use of sensitive personal information if we use that information for purposes beyond what is needed to provide the Services you request or for other reasons specified in the CPPA. As we do not use or disclose sensitive personal information for other purposes without your consent, we do not offer you an option to limit the use of sensitive personal information.

### 10.3 Other U.S. Only State Specific Privacy Rights

If you are a resident of California, Colorado, Connecticut, Maine, Nevada, Oregon, Texas, Utah, or Virginia, you may have specific or additional rights under your state's privacy laws.

Depending on the jurisdiction where you reside and the scope of applicability, you may have certain of the following rights with respect to your personal information:

- Right to know what personal information we collect, how we use and share it, and how long we keep it. The state laws generally require that we provide you information about the categories of personal information we collect and the

purposes for which we collect each category. This Privacy Policy provides details about our collection and usage practices. As described in Section 2 of this Privacy Policy, we collect personal information when you interact with us and use our Services, from third parties, and from the devices you use. Use of certain identity protection Services may require you to provide information such as social security number, driver's license, financial account data, or other information that is considered sensitive personal information under state privacy laws. We retain information only as long as reasonably necessary for business, accounting, tax or legal purposes and then securely delete it. We use the information we collect for business and commercial purposes as those terms are defined by the CCPA. Third parties/service providers we use to perform business functions on our behalf may use information for the same purposes.

- Right to access, delete and correct information. You may have the right to request access to your information, or for us to delete or correct your personal information. Please contact us to request that we delete personal information we have about you, or to correct inaccurate personal information we have about you. Unless we need it for reasons specified or permitted by applicable laws or regulations, we will work with you to delete your personal information accordingly. You may also request access to your information, and we will provide the relevant information to you in a portable and readily usable format.
- Right to limit the use of sensitive personal information. For sensitive personal information that we collect, we will only use or disclose it either with your specific consent when required, or as otherwise permitted by law. As we do not use or disclose sensitive personal information for other purposes without your consent, we currently do not offer you an option to limit the use of sensitive personal information.
- Right to tell us not to use personal information to create profiles about you that we use to inform decisions that have legal or similarly significant effects. We do not use personal information to profile you to further decisions that have legal or similar significant effects.
- Right to tell us not to sell personal information or process it for certain targeted advertising purposes. The laws vary in the way they define sale and certain targeted advertising, but generally, they require that we provide you with the ability to limit activities that involve sharing personal information for monetary or other valuable consideration and using personal information about you from your activity across other websites or apps to target ads to you. You can opt out of certain sharing or processing of your personal information by accessing your privacy preferences page for the applicable Product website. We do not currently respond to Do Not Track signals. We do not knowingly sell or share personal information related to children under 16 years of age.
- Right to appeal a denial of your request to exercise the privacy rights provided by the state law. Some states allow you to appeal a denial of your request to exercise your privacy rights provided by applicable state law. If you are a resident of Colorado, Connecticut, Oregon, Texas, or Virginia and we deny your request to

exercise certain rights pertaining to your personal data, you can appeal the denial of a request to exercise privacy rights by following the instructions listed in the denial communication, by submitting a request through a privacy inquiry to [support+privacy@codetra.co.uk](mailto:support+privacy@codetra.co.uk)

- Right to not be discriminated against. Some state laws ensure that you have the right to not be discriminated against. We do not discriminate against you, or anyone, for your/their exercise of any rights provided to you by applicable state law.

You can exercise your right to know, access, delete, and correct data directly, or, in California, Colorado, Connecticut, Oregon, and Texas, you may appoint an authorized agent to act on your behalf, by submitting a request. You can exercise your right to opt-out of selling and sharing by visiting the applicable privacy preferences page or the cookie banner for the Service you are using. Note we may require you to verify your identity using the processes we describe in an applicable Product dashboard or the privacy choices page before we fulfill your request.

11. Technology Licensing. We occasionally license our technology to third party partners who may integrate it with applications developed and offered by those partners. Our partners, and CODETRA LIMITED, are responsible for those applications and for determining what data is collected by those applications and how it is processed. Please contact the relevant partner and refer to their Privacy Policy to learn more about how those applications process your personal data.

12. Age Restrictions. Our Services are not intended for and may not be used by minors. In this context, minors are individuals under the age of 16 except for our identity and credit monitoring services, which are restricted to those under the age of 18. We do not knowingly collect personal data from minors or allow them to use our Services. If we discover that we have collected personal data from a minor, we may delete such data without notice. Please note that the legal terms under which we make certain Services available may require users to be older than 16 years of age.

13. Privacy Policy Updates. We may update this Privacy Policy from time to time in accordance with this section for reasons such as changes in laws, industry standards, and business practices. We will post updates to this page and update the "Last updated" date above. If we make updates that materially alter your privacy rights, we will also provide you with advance notice, such as via email or through the Services. If you disagree with such an update to this policy, you may cancel your Services account. If you do not cancel your account before the date the update becomes effective, your continued use of our Services will be subject to the updated Privacy Policy.

14. Contact Us. We expect this Privacy Policy to evolve over time and welcome feedback from our users about our privacy practices. If you would like to exercise your rights, have any questions or complaints about our privacy practices, you can contact us using the following details or submit your request to our website <https://codetra.co.uk/>

CODETRA LIMITED - ASTRAVPN

85 Great Portland Street, London W1W 7LT, United Kingdom  
support+privacy@codetra.co.uk