ExaVault Privacy Policy

Last Updated: 1 February 2020

ExaVault Inc. (“ExaVault”) operates web-based and FTP-based services at exavault.com (the “Service”). ExaVault also operates services as EVBackup, a standards-compliant offsite backup service, at evbackup.com. It is ExaVault’s policy to respect your privacy regarding any information we may collect while using our Service. This privacy policy describes the choices available to you regarding our use of the personal information we collect and how you can access and update this information. As a California Corporation, ExaVault complies with the California Consumer Privacy Act. ExaVault also complies with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and the United Kingdom. ExaVault has certified that it adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability. If there is any conflict between the policies in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/

Information We Collect

We collect many different types of information, depending on how you use our service:

- We collect the actual contents of the files uploaded to your ExaVault account ("Customer Data").
- Additionally, we collect "metadata" about your Customer Data that is distinct from the actual content itself ("Customer Metadata"). Customer Metadata includes file and folder names, creation and modification dates, permissions, and size information.
- We also collect metadata about your account overall, not tied to any specific file (“Account Metadata”). Account Metadata includes general account settings, users and their associated data (passwords, access restrictions, etc.), group settings and customer brand data (name, logo, etc.).
- We also collect usage information customarily logged by web and FTP server software, including the date and time of your visit, the originating IP address, the pages and images requested, and other similar types of information. We also get usage data from third parties such as Google Analytics, who may place tracking pixels our site. Collectively, we call this "Usage Data".

- We collect information from those who communicate with us via e-mail or our website for example to ask a question about our product ("Correspondence Data").
- We collect information provided by customers about themselves and their users, such as your name and email address provided during account registration, payment information, and the names and emails of users on your account ("Registration, Billing, and Administration Data").

How Information is Used

- "Customer Data" is stored securely and may only be accessed by users who have been given the appropriate permissions to that Customer Data by someone with administrative permissions on the account. We will not access this data for any other purpose, except as provided below.
- "Customer Metadata" is used by our software systems to provide the Service and may be displayed, subject to our permissions controls, to users on the account.
- "Usage Data" and "Correspondence Data" is used to help us understand how the Service and our websites are being used and to help us improve our websites and the Service.
- "Registration, Billing, and Administration Data" is used for billing purposes and to notify you about important service-related issues. ExaVault uses a third-party payment processor and Registration, Billing, and Administration Data will be sent on to such payment processor. Registration, Billing, and Administration Data will also be used to communicate with you regarding the Service. We communicate such things as announcements of new features, changes to Terms of Use/Privacy Policy, requests for feedback on the quality of the Service, information about pricing changes or systems outages, and other Service-related announcements. We may use a third-party service for purposes of sending these communications, and so names and email addresses that you provide us may be transferred to such a third-party service. After you stop using the service, we may use such emails to communicate offers to you to resume use of the service; all such communications will provide you with an opportunity to opt out of future communications.
- Unless you request otherwise, we may use the name of your company and screenshots from your public website in advertisements promoting ExaVault.
- All information may be disclosed when legally required to do so, at the request of governmental authorities conducting an investigation, to verify or enforce compliance with the Terms of Use and policies governing the Service and applicable laws or to protect against misuse or unauthorized use of the Service. We also may be required to disclose an individual’s personal information in response to a lawful request by public authorities, including to meet national security or law enforcement requirements.

- If we ever were to engage in any onward transfers of your data with third parties for a purpose other than which it was originally collected or subsequently authorized, we would provide you with an opt-out choice to limit the use and disclosure of your personal data.

Our Access To Your Data

- Except as required by law, the only other parties with whom ExaVault might share information we collect are: (a) our contractors and service providers (e.g., payment processor, email list provider) all of whom are bound to terms of confidentiality that are is least is stringent as those stated in this privacy policy, and such sharing only occurs as described in this Privacy Policy; or (b) other parties as authorized in this Privacy Policy or the Terms of Service (e.g., to administrators as part of "Registration, Billing, and Administration Data") or at your direction (e.g., sharing files with others).
- We have implemented controls designed to prevent our employees or contractors from improperly using your Customer Data for purposes other than those set forth in this Privacy Policy. Our employees and contractors will not access your Customer Data unless explicitly authorized to do so by you, e.g. as part of troubleshooting an issue with your account.
- However, as is reasonably necessary to facilitate provision of the Service, employees and contractors of ExaVault may have access to your Customer Metadata, Account Metadata (other than passwords), Usage Data, Registration, Billing, and Administration Data, and Correspondence Data, and may use that to communicate with you or improve the service. For example, we may use the total amount of data you've stored to recommend you switch to a higher or lower plan tier.

Technology

- Wherever possible, browsing sessions to the Service are secured with SSL, to prevent eavesdropping, tampering, and message forgery. If SSL is enabled, you will see a lock icon in your browser.
- If you connect via FTP, you may choose to use FTP, FTP-SSL or SFTP. Only FTP-SSL and SFTP are secured, standard FTP is not.
- At your option, you may turn on 'Secure Only Mode', which will reject any non-secure connections to your account. We recommend that you do this.
- Cookies: Use of the Service requires support for cookies, small pieces of data that are stored on your computer's hard drive and transmitted back to the Service with each web page request. A cookie simply identifies your browser to the Service by assigning it

a unique ID number, which enables us to associate your browser session with your account.

California Privacy Notice

ExaVault is committed to compliance with the California Consumer Privacy Act of 2018 (the "CCPA"). ExaVault operates primarily as a "service provider", as that term is defined in the CCPA, because ExaVault stores data on behalf of other "businesses", and ExaVault has agreed (by virtue of Section 4 of the Terms of Service, or a similar provision) not to disclose that information. "Business", for purposes of the CCPA, is a company that collects personal information and controls it. ExaVault is only a "Business" for the information that it collects from its own customers.

Right to To Opt Out of the Sale of Personal Information. Although the CCPA provides a right to opt out of the sale of personal information, you're opted-out by default: ExaVault has not, does not, and will not sell personal information. It is for this reason that ExaVault does not have a "Do Not Sell My Personal Information" link you may see on other companies' websites.

CCPA Right to Know and Right to Deletion Requests. If you are an ExaVault customer, then you have a right to request disclosure and/or deletion of the personal information that ExaVault has collected from you. You may either submit the request via email to privacy@exavault.com or via a support ticket. Such requests will be subject to verification by requiring two or three items of information stored in your account, and a state-issued ID and signed statement under penalty of perjury. Any such verification information which ExaVault did not previously possess shall only be maintained as long as required to comply with the record-keeping requirements of the CCPA.

You can also request: the categories of personal information collected by ExaVault about you; categories of sources from which collection of personal information about you occurs; the business or commercial purpose for collecting personal information; the categories of third parties with whom ExaVault shares personal information; categories of personal information that the business disclosed about the consumer for a business purpose.

ExaVault will not discriminate against customers that have made requests pursuant to their CCPA rights.

Please note that if you are seeking disclosure of your personal information that you believe ExaVault holds on behalf of one of its customers, then it is almost certain that ExaVault will deny the request and refer you to that customer to seek your CCPA rights. This is because

ExaVault is a “service provider” for its customers as that term is defined in CCPA, and not responsible for the CCPA obligations of its customers.

12-Month CCPA Disclosures

The CCPA requires disclosures in a privacy policy, to be updated every 12 months, of the following items. These lists were last updated as of the “Last Updated” date at the top of this page.

- Categories of personal information ExaVault has collected in the preceding 12 months: these are listed at the top of the Privacy Policy under “Information We Collect”.
- Categories of personal information ExaVault has sold about consumers in the preceding 12 months. None, ExaVault does not sell consumer information.
- Categories of personal information ExaVault has disclosed about consumers for a business purpose in the preceding 12 months for a business purpose. ExaVault has only disclosed or used personal information in the preceding 12 months as described in the “How Information is Used” section of this document, and only with those parties listed in “Our Access To Your Data”.

European Union Privacy Notice

- ExaVault is committed to compliance with the EU General Data Privacy Regulation (GDPR).
- If you are a resident of the European Union or the United Kingdom, then you have additional privacy rights which are guaranteed by the GDPR and other EU privacy legislation. The responsibility for effecting those rights varies depending on your relationship to ExaVault:
- The responsibility for effecting those rights varies depending on your relationship to ExaVault:
    - if you are an ExaVault customer, then ExaVault is a “data controller” for information about your account, such as your address, billing information, and other account metadata. For the data stored in your account, ExaVault is a “data processor”, acting at your direction in processing the data.
    - If you are not an ExaVault customer, but you believe that someone else has stored or processed your personal information using ExaVault, then ExaVault would be a “data processor” working for that third party. The party that uploaded your information to ExaVault would be the “data controller” for that data. ExaVault may also act as a data processor to send notifications, including email, to third parties at the direction of its customers, such as when a customer is sharing files with a third party. In this case it is the responsibility of the data

controller (ExaVault's customer, not ExaVault) to obtain consent for this communication.

- If you have questions or concerns about personal information in data for which ExaVault is a data processor (i.e., most data that is uploaded by a user to ExaVault), we encourage you to communicate with the data controller for the data. If you make EU/GDPR rights requests to ExaVault regarding data where ExaVault is the data processor, we will refer any such request to the relevant data controller, who is the party primarily responsible for implementation of those rights.
- For information for which ExaVault is a data controller (e.g., address, billing information, and other account metadata), if you are an EU resident then you have the following rights with respect to that data:
    - You have a right to know what data is being processed, why it is being processed, and how long it will be retained, as described above in "Information We Collect", and "How Information Is Used";
    - You have a right to ask us to correct or delete data that you think is incorrect;
    - You have the right to lodge a complaint with the supervisory authority (for more information, see the next section on US-EU Data Privacy Shield Framework);
    - You have a right to request a copy of the data, although ExaVault may charge you a reasonable fee for it;
    - You have a right to request that we delete this data, although our obligation to completely delete the data may be limited by legal requirements. For example, we will maintain a record that we deleted the data, including a record of your contact information, so that we can demonstrate that it was done at a later date;
    - You have a right to request a copy of the data, although in many cases we will refer you to your account settings page, which holds the majority of this type of data.
- ExaVault acknowledges that individuals have the right to access the personal information/data that we maintain about them, in our function as a data controller. An EU individual who seeks access, or who seeks to correct, amend, or delete inaccurate data, should direct his query to their Client Services manager or email privacy@exavault.com. ExaVault will respond within a reasonable timeframe, and in no event greater than thirty days. Please be aware that we may refer you to the data controller, for data where ExaVault is merely the processor.
- ExaVault's servers are primarily located in the United States, although ExaVault may provide options to use servers in other locations. In order to ensure compliance with the GDPR for transfers to the United States, ExaVault has entered into the U.S.-EU Data Privacy Shield framework, as described below. Our Terms of Service also include a Data Processing Addendum which also provides additional legal structure for this transfer of information to the United States or other jurisdictions.
- ExaVault also uses technical support staff located in non-EU countries outside the United States. ExaVault has entered into confidentiality agreements with all such

personnel. Your information is only transferred to the such countries when our personnel there would access it in response to a technical support request from the data controller (i.e., a ExaVault account owner). Such transfers are governed by the standard contractual clauses, which you agree to as part of the terms of service, and which we have entered into with our support staff to ensure adequate safeguards for such transfers.

- ExaVault has applied reasonable technological measures in order to ensure the security of data stored on ExaVault. You can read more about these technological and operational measures in our public security overview. Because ExaVault does not know what data you upload via the service, it is your responsibility to ensure that those technological and operational measures are appropriate for the categories of data that you are uploading.

U.S.-EU Data Privacy Shield Framework

- ExaVault complies with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and the United Kingdom transferred to the United States pursuant to Privacy Shield. ExaVault has certified that it adheres to the Privacy Shield Principles with respect to such data. If there is any conflict between the policies in this privacy policy and data subject rights under the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/
- ExaVault's accountability for personal data that it receives under the Privacy Shield and subsequently transfers to a third party is described in the Privacy Shield Principles. Pursuant to the Privacy Shield, ExaVault remains liable for the transfer of personal data to third parties acting as our agents unless we can prove we were not a party to the events giving rise to the damages.
- In compliance with the Privacy Shield Principles, ExaVault commits to resolve complaints about your privacy and our collection or use of your personal information transferred to the United States pursuant to Privacy Shield. European Union or United Kingdom individuals with Privacy Shield inquiries or complaints should first contact ExaVault at:

  Client Services Manager
  privacy@exavault.com
  Phone: +1 (510) 500-0245
  ExaVault, Inc.
  344 Thomas L Berkley Way
  Oakland, CA 94612

- ExaVault has further committed to refer unresolved privacy complaints under the EU-US Privacy Shield Principles to an independent dispute resolution mechanism, BBB EU PRIVACY SHIELD, operated by the BBB National Programs, Inc. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit https://www.bbb.org/EU-privacy-shield/for-eu-consumers/ for more information and to file a complaint. This service is provided free of charge to you.
- If your Privacy Shield complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See Privacy Shield Annex 1 at https://www.privacyshield.gov/article?id=ANNEX-I-introduction.
- ExaVault is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

Removing Information

- You may use the Service to delete any of your "Customer Data," and doing so will remove access to such content from our active servers immediately. Your data may remain on our backup servers for a short period of time, but will be automatically removed.
- All of your "Customer Data" and "Customer Metadata" will be deleted from our active and backup servers within 30 days after you cancel your account.

Other Provisions

- Your use of the Service is governed by a Terms of Service, which will prevail in the event of a conflict with this document.
- This Privacy Policy does not describe information collection practices on other sites, including those linked to or from the Service.
- We use third parties to facilitate our business, such as server hosting, file hosting, and payment processing. In connection with these offerings and business operations, our service providers may have access to your information in connection with these business activities. Where we utilize third parties for the processing or storing of any information, we have ensured that they will fully comply with this Privacy Policy.
- Google Analytics: We use Google Analytics, a web analytics service provided by Google, Inc. ("Google"). Google Analytics uses cookies and other methods to help us study usage patterns on the Service. Information generated from your use of the Service will be transmitted to and stored by Google on servers in the United States. Google will use this information for the purpose of preparing reports regarding

aggregate use of the Service. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf.

- If the ownership of all or substantially all of ExaVault, Inc., or individual business units associated with the Service, were to change, your user information may be transferred to the new owner so the service can continue operations. In any such transfer of information, your user information would remain subject to the promises made in this Privacy Policy. In the event of such transaction, we will alert ExaVault paying customers of such change via E-Mail, and provide an opportunity to cancel or change your service.

Changes to this Privacy Policy

- ExaVault, Inc. reserves the right to change this Privacy Policy at any time by posting a new Privacy Policy at this location and alerting ExaVault paying customers of such change via E-Mail. Any change(s) to this Privacy Policy will take effect thirty (30) days after such changes have been posted. Your continued use of the Service following such changes will indicate your acceptance of those changes.
- This document was last updated according to the date at the top of this page.

ExaVault, Inc. regularly reviews its compliance with this policy. Questions regarding the Privacy Policy should be sent by e-mail to us at privacy@exavault.com.