Dashlane Privacy Policy

Our Privacy Policy is below. You have to accept it to use our software, but we know it can be hard to follow. To help you understand what you are agreeing to, each section starts with a short "non-legal" summary. The summaries are not technically part of the Policy.

LAST UPDATED: December 5, 2023

1. INTRODUCTION

Summary:
This Policy describes how we obtain and use personal data (which can be used to identify a specific individual) and anonymous data (which can't) about our users. Certain parts of the Policy apply only to specific users, like people who use Dashlane on an employer provided plan). We may change this Policy at any time by posting the revised Policy here. We will also notify current users of major changes through email or in-app messaging. While we need certain personal data to provide the Services, we try to collect only what we need. We will remove personal data about children who are not authorized users (e.g., part of a Family Plan) when requested. ***Because of our zero-knowledge architecture, we do not and cannot know what information you store on the Services.***

a. *General*. This Privacy Policy (the "**Policy**") describes how Dashlane, Inc. and its affiliates ("**Dashlane**" or "**we**") collects, uses and shares information about visitors to our website at www.dashlane.com (together with its subdomains, such as the Dashlane blog, the "**Site**") and users of our web extensions and mobile and web applications (each an "**App**" and, collectively, the "**Apps**"). The Apps and the Site together are the "**Services**." "**You**" or "**user**" refers to anyone who uses the Services or visits the Site. Capitalized words used but not defined in this Policy have the meanings provided in our Terms of Service (the "**Terms**").

b. *Personal and Anonymous Data*. "**Personal Data**" means information that, either alone or when combined with other information, identifies an individual, such as name, mailing address, email address, IP address, or telephone number. "**Anonymous Data**" means data that cannot be used to identify individuals. We collect and use both Personal and Anonymous Data as described below.

c. *Privacy Laws*. An increasing number of laws like the California Privacy Rights Act ("**CPRA**") and the European Union's General Data Protection Legislation ("**GDPR**") govern how entities collect, store, and use Personal Data (collectively, "**Privacy Laws**"). Privacy Laws grant individuals defined rights to know how companies use their Personal Data, and to limit those uses. As much as possible, we design our policies to comply with the most protective Privacy Laws, and we apply these policies to all users, whether or not the laws technically apply to them. Section 8 of this Policy specifically addresses rights users may have over their Personal Data that are at the heart of most Privacy Laws.

d. *Business Users.* Certain clearly labelled sections of the Policy only apply to users who access the Services under a plan provided by their employer or similar entity (each, a "**Business User**").

e. *Changes*. We may change this Policy at any time. When we do so, we will post the updated Policy on this page and, if the changes are material, inform users through email or in-App messaging.

f. *Children*. The Services are not directed to children, but children can use the Services as members of a Family Plan. If you become aware that a child (based on the jurisdiction where the child lives, which in the United States means someone under 13) has provided Personal Data without parental consent, please contact our help center amd we will promptly remove the information from our systems.

g. *Why Do We Need Your Personal Data*? We need certain Personal Data to provide the Services. You will be asked to provide this information to download and use the Apps. This consent, which you may withdraw at any time, provides the legal basis we need to process your Personal Data. You are not required to provide Personal Data, but we may not be able to provide the Services or respond to inquiries if you don't.

h. *Secured Data*. This Policy primarily addresses data that Dashlane uses to process payments, troubleshoot issues, administer accounts, etc. This is distinct from the information our users store on our Services ("**Secured**

Data"). Dashlane cannot access Secured Data; it is encrypted with keys that are unique to each user, that we do not have, and there is no "backdoor" or equivalent mechanism that lets us access Secured Data. See our Security Whitepaper for detailed information.

2. WHAT PERSONAL DATA DOES (AND DOESN'T) DASHLANE COLLECT?

Summary:
California's Privacy Laws require that we disclose the types of Personal Data we collect. We do not collect all of it for every user – we don't need Billing Data for Dashlane "Free" users, for example – and the following sections provide more detail on what we collect and how we use it.

California requires that we disclose whether we collect Personal Data in each of the categories below. This is a general overview of the types of Personal Data we collect; we do not collect all data for every user. See the following sections of the Policy for details about how we obtain and use this information.

- *Identifiers* include name, email address, and mailing address, as well as government-issued identifiers like a driver's license or social security number. We need an email address from every user to create an Account. Except in very rare circumstances (when we need to verify your identity in connection with account restoration) we never ask for government IDs or similar information from users.
- *Customer records* overlap with Identifiers (name, address, IDs) but also include things like payment, medical, and insurance information. Obviously, we process credit card, Paypal, or bank account information as directed for paid accounts (but we do not keep it following processing). Internally, we assign each user auniquue ID that is used only within Dashlane systems.
- *Characteristics of protected classifications* such as race, ancestry, sexual orientation, marital status, etc. **We do not collect this information**.
- *Commercial information* such as records of personal property, products or services purchased, or purchasing or consuming histories. We collect information about payment history (where applicable) and what Dashlane plan is associated with a user or account.
- *Biometric information*. **We do not collect this information.** If you use biometrics to login onto the Service, this information is only used on the device.
- *Internet or other electronic network activity information* such as browsing history, search history, or information regarding a consumer's interaction with a website, application, or advertisement. We collect information about which pages on our Site a visitor interacts with, as well as what of our advertisements (if any) they saw prior to visiting our Site. We collect IP addresses as noted below. **We do not collect browser information from Apps**. While the Apps themselves recognize sites and can correlate information in your Secured Data to the sites and applications you visit, this occurs locally, and none of this information is reported to, or stored on, our servers.
- *Geolocation data*. For B2C users, we collect the originating IP and the most recent 45 days of IP activity. We retain up to one year of IP activity for B2B users.
- *Audio, electronic, visual, thermal, olfactory, or similar information*. We record sales, support, and user research calls, which may be audio only or audio and video, with affirmative consent. We may retain this information for up to 2 years.
- *Professional or employment-related information*. We collect this information for administrators of B2B accounts and prospective B2B customers.
- *Education information not considered publicly available*. **We do not collect this information**.
- Inferences that can create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, or aptitudes. **We do not collect this information**.
- *Sensitive personal information*. This includes many items covered in the above categories, such as financial or medical account information, government ID information, racial and other "protected"

demographic information, and biometric information. Except for payment information as noted above, **we do not collect this information**.

3. HOW DOES DASHLANE OBTAIN DATA?

Summary:
We get data from you (e.g., when you create an Account or pay for a Subscription), from others (e.g., when you are invited to use Dashlane by your employer), automatically from the Apps or through cookies (e.g., the region you are accessing the Apps from), and from third parties (such as tools that analyze performance of the Services). Personal Data we collect includes your email and (for Subscriptions) billing information, although complete payment information is only stored by our payment processors. We use technology, including cookies, to collect usage data. Additional information is available in our Cookie Policy.

We collect information in the following ways:

a. *Information You Provide.*

- Registration Data. You must create an Account to use an App, and to do so you must provide a valid email address that will be used as your login to the Services (unless you are a Business User logging in via single sign on "**SSO**"). You may also provide a phone number (to set up two-factor authentication) and / or an additional email (for example, if you lose access to the email used to login to your Account). *The only Personal Data required to open a Dashlane Free account is your email*. For paid Accounts, users must provide billing data as specified below. For Dashlane Business or Dashlane Teams Accounts "**B2B Accounts**," registration data includes the business name, mailing address (if paying by invoice), and administrator contact information. **It is critical to keep registration data current**. We must be able to verify the Account owner to respond to user support requests. If you lose access to the contact email or phone number associated with your Account (if applicable), you may be locked out of your Account, and we may be unable to help you. We store registration data for up to 30 days after Account deletion.
- Billing Data. We use third-parties to process payments made through the Site. We may store partial payment information (such as the expiration date and last four digits of a credit card) for tax compliance and user support purposes. We may be able to access the name, address, and phone number associated with a payment method on a payment processor's service, but this information is only stored by the processor. We never have complete payment information for Accounts, nor do we receive or store billing data if you pay for a Subscription through the Google Play or Apple App Stores ("***App Stores***"). Billing data is retained for up to 30 days after Account deletion.
- Master Password. Except for Dashlane Business users using SSO, each user must create a "**Master Password**," which is used to access their Account and generate the encryption keys that protect their Secured Data. The more secure a Master Password is, the safer Secured Data will be. Apps do not store Master Passwords locally unless directed to by the user. If you do so and your device is stolen or compromised, your Secured Data may be exposed. Dashlane never has access to Master Passwords.
- Secured Data. Our Apps let you manage digital identity data, including sensitive information such as credit card numbers and site or application credentials. This, and everything else you store on the Apps, is Secured Data. Secured Data is always encrypted when transmitted and stored and may only be decrypted locally on an authorized device. **Dashlane cannot access Secured Data on our servers because we do not have the encryption keys as noted above**. See our Security Whitepaper for details.
- Support and Correspondence. You may provide Personal Data in connection with customer support requests and inquiries from our Site. Customer support histories are maintained for up to 30 days after Account deletion.
- Feedback. If you provide Feedback, including reviews posted on social channels, App Stores or sites like Trustpilot, or suggestions made in connection with market research, we may use Personal Data provided with the Feedback to respond to you. We may use Feedback without limitation as described in the Terms.

- Requests for Product Information. Certain information intended to inform potential customers of Dashlane's commercial offerings ("**Business Prospects**") is available from our Site only after providing a verified email.
- Other Data. We may also collect other types of information in the manner disclosed by us when the information is collected.

b. *Data You Provide About Others.* The Services let you invite others to try the Apps or join your Account. If you do this (or are invited this way), Dashlane will store the invitee's email address and the message sent to them to follow up (and, if applicable, credit the referrer with a referral bonus). We will let the invitee know who referred them, and let them request that their information be deleted from our systems. The referrer or invitee may contact the Support Center to request removal of this information.

c. *Data Collected by Technology.*

- IP Address. We collect the IP address used to create a new Account, and the IP addresses from which users access the Services. This data is used to deliver and improve the services and for compliance purposes (e.g., using the region associated with an IP address to display local regulatory notices). The creation IP is kept for up to 30 days after Account deletion. Access IPs are kept for 45 days for B2C accounts, and for up to one year for B2B accounts.
- Device and Browser Data. We automatically log the following information (as applicable) when you access the Services or visit the Site: operating system name and version, device identifier, browser type, and browser or device language. Some of this data is collected using cookies, as explained in the Cookie Policy. This data is used to secure your Account, ensure the Site and Services are presented in the correct language and optimized for your device, and facilitate customer support. This data is not deleted, but is anonymized within 30 days of Account deletion.
- Usage Data. We use logs to collect data about the use of the Services ("**Usage Data**"). We maintain two types of Usage Data:
    - "**Event Data**" records the Apps' internal functions (e.g., what features are enabled, how many credentials are stored in Secured Data), and is used to provide relevant information and support to the user and to deliver, analyze, and improve the Services. Event Data does not include information about how the Services interact with third parties (e.g., while we know how many passwords a user has, we do not know which sites or services those passwords are for). After an Account is deleted, Event Data is retained, but is fully anonymized (even if the same user created a new Account, Event Data from the old Account could not be associated with the new one). Retention of anonymized Event Data is necessary to maintain accurate historical records of the use of the Services.
    - "**Behavioral Data**" is information about what users do outside of the Services (e.g., sites where autofill is used to sign in; what sites or apps a user has credentials for in their Secured Data). Behavioral Data is critical to the Services' proper operation – Apps must recognize the site a user is logging into to populate the credentials, for example. Certain Behavioral Data is available to authorized administrators of B2B Accounts (each, a "**Client Admin**") on an individual basis to enable Client Admins to improve Client security (e.g., Client Admins can see whether an individual user has compromised credentials), but is only available to Dashlane on a fully anonymized basis (e.g. Dashlane can see what percentage of all users have credentials for a specific site, but not whether any individual user has credentials for that site). Dashlane cannot associate Behavioral Data with any individual User.

  Certain Dashlane personnel can access Event Data to analyze the use of the Services and provide user and technical support. Both Event Data and Behavioral Data are used by the Services to automatically generate context-appropriate alerts (e.g., account set-up notices), and to generate aggregated data.
- Aggregated Data. We derive additional information about the use of the Services by aggregating Usage Data (e.g., number of users within a particular jurisdiction, most popular features). Aggregated data is Anonymous Data, is owned by Dashlane, and is primarily used to help analyze and improve the Services.

- Cookies. As described in our Cookie Policy, we use cookies and similar technologies to recognize you and/or your device(s) and provide a more personal and seamless experience when interacting with the Site and Services. Cookies that are not essential to the operation of the Services can be disabled at any time here.

d. *Data obtained from Third Parties.*

- Business Users. If you are a Business User, your Client Admin may provide your email or SSO information as part of Account creation.
- Service Providers. We receive information about users from our service providers (such as when validating an Account with a payment processor or when monitoring App performance with analytics services). We may also obtain user information from publicly available sources like social media accounts, review sites, and forums. We obtain information about Business Prospects from data enrichment services. We carefully review the legal terms and business and security practices of all service providers from which we receive this information to ensure that they comply with applicable laws and this Policy.

4. HOW DOES DASHLANE USE PERSONAL DATA?

Summary:
We use Personal Data to validate your Account, provide the Services and support, communicate with you, and coordinate marketing efforts. We do not perform any automated decision making or profiling using Personal Data.

a. *General.* Dashlane uses Personal Data to provide and promote the Services and respond to your requests, including to:

- Establish, maintain, and secure your Account.
- Identify you as a user and provide the Services you request.
- Perform fraud detection and authentication.
- Measure Usage Data to improve the Services and your interactions with them.
- Send you administrative notifications, such as payment reminders or support and maintenance advisories. You will receive these notices even if you opt out of marketing communications.
- Provide you with interfaces and options you request or as required by the jurisdiction from which you access the Services.
- Provide personalized information by identifying whether you have used specific features within the Services, visited pages on our Site, or seen one of our advertisements.
- Respond to support inquiries and other requests.
- Promote the Services or send you other Dashlane marketing information, including announcements about offerings from selected Dashlane partners. Where required by local laws, users must opt-in to receive marketing communications. Otherwise, marketing communications are activated by default, but users may always opt out of them at any time.
- Manage advertising efforts on third-party sites and platforms as described below.

b. *Automated Decision Making and Profiling.* We do not use Personal Data for automated decision-making.

5. HOW DOES DASHLANE SHARE PERSONAL DATA?

Summary:
We never sell our users' Personal Data. We share Personal Data with service providers who are contractually obliged to comply with Privacy Laws and who only have access to the data they need to provide the relevant services. The Services allow you to share Secured Data (which may include Personal Data) with others as you direct. We share hashed user emails and device ids with advertisers to refine advertising efforts (e.g., so active users are not shown Dashlane ads). We may share Personal Data with our affiliates, all of whom are bound by this Policy, or with an acquirer if Dashlane is sold or merged. Dashlane Client Admins have access to relevant Usage Data (e.g., about the

"business" spaces of users of that Account). Finally, we may disclose Personal Data where required by law or where we believe it is necessary to protect our rights or the Services.

Dashlane will never sell your Personal Data (as "sell" is normally defined – see Section 8 for information about "sales" as defined in California) or use it except as stated in this Policy. We share your Personal Data in the following circumstances:

- Third Parties You Designate. You may use the Services' "sharing" feature to make certain Secured Data available to others. While this data is transferred through our servers, we do not have access to it, as noted elsewhere in this Policy.
- Service Providers. We share Personal Data with service providers solely as required to provide the Services, including to create Accounts, provide support, process payments, or enable communication between you and Dashlane (for example, Personal Data related to customer support requests is available to our support agents on Zendesk). We review the security and data privacy practices of all service providers to ensure that they comply with applicable laws and this Policy. Secured Data stored by our data hosting provider (AWS) is always encrypted as described above. The Subprocessors List discloses what service providers have access to Personal Data in connection with our delivery of the Services.
- Marketing. We provide hashed emails and/or device IDs to service providers to optimize our advertising efforts (e.g., ensuring that current users are not shown Dashlane ads on other sites). These providers are prohibited from using this information for any other purpose, including augmenting profiles they maintain. We provide hashed emails of Business Prospects to data enrichment providers to improve marketing efforts.
- Affiliates. This Policy applies to all entities that are owned by, or under common control with, Dashlane, Inc. ("**Affiliates**"). We share Personal Data among Affiliates as required to provide the Services and respond to requests. Certain Affiliates are in the United States, where privacy and related laws are not deemed adequate by European regulators to hold and protect Personal Data. To offer the levels of protection required, we have GDPR-compliant Data Processing Addenda or equivalent documents in place among our EU and US Affiliates, in addition to the other measures indicated below.
- Dashlane Client Admins. Business Users have access to two "spaces" in their Apps: a "business space" to store Secured Data related to their work, and a "personal space" for anything else they want to store on the Services. The Services allow Client Admins to view information about the use of Services by the Business Users associated with their Account, including detailed information about the use of the business space. This information includes Event Data, as well as certain Behavioral Data on an individual basis. For example, a Client Admin can see the Password Health scores of Business Users associated with their Account, which sites or services an individual Business User has stored credentials for in their business space, and whether those credentials have been compromised.
- Corporate Restructuring. If Dashlane or its business or assets are acquired by, or merged into, another company, that company will then possess the Personal Data we hold, and will assume our rights and obligations under this Policy. Accordingly, we may share Personal Data in connection with any such transaction. Personal Data and other information may also be transferred as a business asset in the event of Dashlane's insolvency, bankruptcy, or receivership.
- Other Disclosures. We will inform you of any other disclosures of your Personal Data and obtain your consent prior to such disclosure. However, regardless of your choices regarding Personal Data, Dashlane may disclose your Personal Data (a) where required to comply with law enforcement directives, applicable laws or governmental orders; or (b) if we believe in good faith that doing so is necessary to protect our rights, those of other users, or the Services. However, because of our zero-knowledge architecture, we are unable to provide Secured Data, even if we are subject to a valid order. To the extent permitted by law, we will inform affected users of legally-mandated disclosures of Personal Data.

6. DATA SECURITY AND INTERNATIONAL TRANSFER

Summary:
We strive to protect all data in our possession, including Personal Data, through a variety of means, and we continually work to improve and update these practices. However, we cannot and do not guarantee the security of Personal Data we process. Personal Data may be transferred to jurisdictions with less strict privacy laws than those in your home country, including the U.S., but we use technical and other measures that comply with applicable Privacy Laws to protect Personal Data when processed in the U.S.

a. We use robust physical, organizational, technical, and administrative measures to safeguard all data we hold or process, and we regularly reassess and revise our policies and practices to improve security. While we go to great lengths to protect your data, no method of data transmission or storage is totally secure; therefore, we cannot guarantee the security of data in our control. If you believe your data may have been compromised by us or the use of the Services, please contact our help center immediately.

b. Your information, including Personal Data that we collect from you, may be transferred to, stored by, and processed by us, our Affiliates, and service providers outside your home country, including in the United States, where data protection and privacy regulations may not offer the same protections as in other parts of the world. When we do so, we take all legally mandated steps designed to ensure that all Personal Data we or our service providers process (regardless of where it originates) is properly protected. By using the Services, you agree to the transfer, storing, or processing of your data in accordance with this Policy.

7. HOW CAN YOU CONTROL YOUR DATA?

Summary:
You can edit your Personal Data and adjust your privacy and data preferences via the "Account" or "Settings" sections of the Apps. If you currently receive marketing emails but no longer want to, you may unsubscribe in any such email. Even if you do so, we will still send you operational and transactional emails (e.g., renewal notices). Uninstalling Apps from your devices will remove all data associated with the Apps from that device. Removing your Apps does not delete your Account. To do that, see the instructions here. Even if you are not subject to any Privacy Laws, you may also use the processes described in Section 8 to control your Personal Data.

a. *Changing Your Information and Privacy Settings*. You can access and modify Personal Data associated with your Account, and modify your privacy and data preferences, through the "My Account" or "Settings" sections of the Apps. Contact our help center if you need assistance.

b. *Email Communications*. With your consent, we will periodically send you emails promoting the use of the Services, including tips on using the Apps, or highlighting offerings from select Dashlane partners. You can opt out of these emails by following the unsubscribe instructions included in each email, or by changing your privacy and data settings in the Services. You may also request removal through our help center. Unsubscribing from marketing communications will not affect operational and transactional communications, including breach notices and other alerts in the Apps, renewal emails, etc.

c. *Applications*. You can stop all collection of information by an App by uninstalling that App. You may use the standard uninstall process for the relevant device or platform. Uninstalling an App does not delete your Account. To do that, see the instructions here.

8. PRIVACY LAW RIGHTS

Summary:
*Users subject to Privacy Laws have certain rights regarding their Personal Data, including the right to access and modify Personal Data held by providers (like us), and to have providers "forget" Personal Data that is no longer relevant. Most of these rights must be accessed from the privacy and data preferences in the Services, but you may always contact us for assistance. We will **never** provide worse services to, or in any way punish anyone who chooses to exercise these rights. We strongly support the intent behind these laws and will do our best to honor requests to exercise these rights even if they do not technically apply to you.*

a. *Data Controller*. For the purposes of the GDPR, where we are acting as a controller, the controller is Dashlane SAS of 21 Rue Pierre Picard, 75018 Paris, France. Inquiries regarding the processing of data subject to the GDPR may be sent to our data protection officer at dpo@dashlane.com.

b. *Sale and Sharing of Personal Data*. We never exchange Personal Data for money or any other consideration (e.g., trade it for free services). However, when you click on an ad that sends you to Dashlane, we send a unique identifier to the referring site so they can receive credit for the referral. If this is not a "sale" as defined under California's Privacy Laws, it is definitely included in "sharing." While the information we send does not include any Personal Data, the fact that you clicked on a link and visited Dashlane may be added to your profile by the ad publisher. This is all done on the Site with "Publisher Cookies" (as defined in our Cookie Policy) and opting out of the sale and sharing of your Personal Data will turn these cookies off.

c. Individuals subject to Privacy Laws have some or all of the following rights with respect to their Personal Data that we process. As noted elsewhere, we will honor these requests when made my any user, subject to the requirements of the relevant Privacy Laws (if applicable). For example, a Business User who is subject to the GDPR may request that we delete their information, but in that situation the company whose Account the user is associated with is the "Controller" of that Personal Data, and we are obligated to inform the relevant Client Admin and follow their instructions.

- Withdraw Consent: You may withdraw your consent to our processing of your Personal Data, in whole or in part (i.e., for marketing purposes). Certain Services may be ineffective upon opt out.
- Access / Request Information: You may access the Personal Data we hold about you at any time via your Account or by contacting us directly.
- Modification: You may modify incorrect or outdated Personal Data we hold about you at any time via your Account or by contacting us directly.
- Erase and Forget. In certain situations, for example when Registration Data we hold about you is no longer relevant or accurate, you can request that we erase it. If you delete your account, all Personal Data will automatically be erased within a week of the date of deletion. **Because of the sensitive nature of Secured Data, we will never delete a user's account ourselves: accounts MUST be deleted by the user or the "controller" or equivalent entity.**
- Portability: You may request a copy of your Personal Data and may always move it to other entities as you choose. The Services allow you to export Secured Data at any time.

d. If you want to exercise any of these rights, please submit the request via the "Privacy and Data Settings" page accessible from the "Account" or "Settings" sections of the Apps (if you cannot do so directly from within these sections). If you need assistance, please visit our Support Center or write us at the address below. In your request, please make clear: (i) **what** Personal Data is concerned; and (ii) **which rights** you want to enforce. For your protection, we may only fulfill requests with respect to the Personal Data associated with the email address you send your request from, and we may need to verify your identity before doing so. We will comply with your request promptly, but in any event within the legally mandated timeframes (e.g., thirty (30) days for the GDPR and forty-five (45) days for the CPRA). If you are not subject to Privacy Laws, we nonetheless try to fulfil all requests within 45 days. We will retain limited Personal Data for recordkeeping purposes or to complete transactions that you began prior to requesting certain requests.

e. We do not and will not discriminate against any user (such as by providing worse service or charging more for them) who exercises any of the above rights.

9. CONTACT INFORMATION; COMPLAINTS

If you have questions, concerns, or complaints about this Policy or our data collection or processgin practices, or if you want to report any security violations, please contact our https://support.dashlane.com/hc/en-us/articles/4516905332370, email legal@dashlane.com, or write the address below:

Dashlane, Inc.
Attn: Legal

44 West 18th Street., 4th Fl.
New York, NY 10011

You may also email either dpo@dashlane.com or legal@dashlane.com.

Swiss, EU and UK Users Only. We hope to promptly resolve any complaint brought to our attention, however if you feel that your complaint has not been adequately resolved, you may always contact your local data protection supervisory authority, a list of which is available here.