Dashlane Privacy Policy

Our Privacy Policy is below. You will have to accept it if you want to use our software, but we know it can be hard to follow. We want you to understand what you are agreeing to, so each section starts with a short "non-legal" summary. The summaries are not part of the Policy but are provided as an aid to understanding it.

LAST UPDATED: FEBRUARY 10, 2021

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, which are clearly labeled, apply only to some users (e.g., those in the EU or California). We may change this Policy at any time by posting the revised Policy here. We will notify current users of major changes through email, in-app notifications, or otherwise. 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.

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 mobile, desktop and web applications (each an "**App**" and, collectively, the "**Apps**"). The Apps and the Site together are the "**Services**." "**You**" or "**user**" refers to any user of the Services or visitor to the Site. Capitalized words used but not defined in this Policy have the meanings provided in our Terms of Service (the "**Terms**").

b. *Region Specific Provisions*. Parts of the Policy apply only to people subject to geographically defined privacy laws like the California Consumer Privacy Act ("**CCPA**"), the European Union's General Data Protection Legislation ("**GDPR**") and Brazil's LGPD. These provisions are clearly labeled. Otherwise, the Policy applies equally to all users of our Services.

c. *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 existing users through email or the Services.

d. *Children*. The Services are not directed to children. However, children who are invited to use the Services by a parent or guardian (under a Family Plan or equivalent) may do so. 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 us with Personal Data without parental consent, contact our help center. We will promptly remove such information from our systems.

e. *Personal and Anonymous Data*. As used in this Policy, "**Personal Data**" means information that, either alone or when combined with other information we hold, identifies an individual, such as name, mailing address, email address, IP address, or telephone number. "**Anonymous Data**" means data that, alone or combined with other information available to us or a third party with whom the data is shared, does not permit identification of an individual. We collect and use both Personal Data and Anonymous Data as described below.

f. *Why Do We Need Your Personal Data*? We need certain Personal Data to provide the Services. You will be asked to provide this information — and must agree to this Policy and the Terms —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 the Personal Data that we request, but we may not be able to provide you with the Services or respond to your inquiries if you don't.

2. PARTICULARLY IMPORTANT INFORMATION (CERTAIN JURISDICTIONS)

a. *(EUROPEAN, BRITISH, AND BRAZILIAN USERS).*

i. **Who We Are**. For the purpose of the GDPR, LGPD, and other legislation that requires the identification of a data controller of your Personal Data, the controller is Dashlane SAS of 21 Rue Pierre Picard, 75018 Paris, France. You may contact our data protection officer at dpo@dashlane.com.

ii. **Must Read Sections***:* Please carefully review the sections entitled "Data Security and International Transfer" and "Your Rights Regarding Personal Data."

b. *(CALIFORNIA AND NEVADA USERS).*

i. **Sale of Personal Data.** You may opt out of all sales of your Personal Data on the Do Not Sell my Personal Information page. **We never exchange Personal Data for money or any other consideration (e.g., trade it for free services)**. However, the CCPA's broad definition of "sale" may include situations where conversion data is sent to referral advertisers (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). 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 of your Personal Data will turn these cookies off.

3. HOW DOES DASHLANE OBTAIN DATA?

Summary:
We get data that you provide (such as when you create an Account or pay for a Subscription), that others provide (when you are invited to use Dashlane by your employer), that we obtain automatically from the Apps or through cookies, and from third parties. Personal Data we collect includes your email (used to create an Account) and (for Subscriptions) certain billing information, although complete payment information is only stored by our payment processors. ***We do not and cannot know your Master Password and, because of that, we do not and cannot know what Secured Data you store on the Services****. We use technology, including cookies, to collect usage data that we use to provide and improve the Services. 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. *The only Personal Data required to open a Dashlane Free account is your email*. We store registration data until seven (7) days after you delete your Account. For paid Accounts, users must provide billing data as specified below. For B2B Accounts, registration data includes the business name, mailing address (if paying by invoice), and administrator contact information, and may include the business email addresses of users. **It is critical to keep registration data current**. We must be able to verify that you are the Account owner to respond to certain customer service requests. If you lose access to the validated email address associated with your Account or a phone number used to validate your identity (if applicable), you may be locked out of your Account, and we may be unable to help you.
- Billing Data. We use third party service providers to process payments made through the Site. We store the expiration date and last four digits of your 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 your complete credit card information, nor do we receive or store any billing data if you pay for a Subscription through the Google Play or Apple App Stores ("***App Stores***"). Billing data is retained until seven (7) days after you delete your Account.
- Master Password. Except for members of B2B Accounts that use single sign on ("**SSO**") to access the Services, each user must create a "**Master Password**," which is used to access their Account and generate the encryption keys that secure the information they store in the Apps ("**Secured Data**" as further defined below). Ultimately, the more secure a Master Password is, the safer Secured Data will be. Dashlane's Zero Knowledge technology ensures that we do not and cannot know our users' Master Passwords or the data

used to generate SSO encryption keys, so we cannot access Secured Data. There is no backdoor or master key; even if a hacker somehow obtained all the Secured Data on our servers, they would have to hack each Account separately. Apps do not store Master Passwords locally unless specifically directed by the user. If you direct an App to retain your Master Password and your device is stolen or compromised, your Secured Data may be exposed.

- Secured Data. Our Apps let you manage digital identity data, including sensitive information like 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. Secured Data on Dashlane servers cannot be accessed by Dashlane because we do not have access to the encryption key as noted above. See our Security Whitepaper for detailed information about how Dashlane protects your Secured Data.
- Support and Correspondence. You may provide Personal Data in connection with user support requests and inquiries from our Site. User support histories are maintained until seven (7) days after the associated Account is deleted.
- Feedback. If you provide us with Feedback, including reviews posted on App Stores or sites like Trustpilot, or suggestions made via Productboard and other direct research or outreach, we may use Personal Data provided with the Feedback to respond to you. We may use Feedback without limitation as described in the Terms.
- 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. If you do this (or are invited this way), Dashlane will store the invitee's email address and the message sent to them in order to follow up (and, if applicable, credit the referrer with any referral bonus or equivalent). We will let the invitee know who referred them to Dashlane, and let them request that their information be deleted from our systems. The referrer or invitee may contact the help center to request removal of this information.

c. *Data Collected by Technology.*

- Device and Browser Data. We automatically log the following information (as applicable) when you access the Services: operating system name and version, device identifier, browser type, browser language, and IP address. Some of this data is collected using cookies, as explained in the Cookie Policy. This data is used to secure your Account, ensure the Services are presented in the correct language and optimized for your device, facilitate customer support, and for tax and compliance purposes (e.g., using the region associated with your IP address to display local regulatory notices). This data is kept in our system until seven (7) days after you delete your Account.
- 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, which is linked to Registration Data, and Behavioral Data**,** which is fully anonymous.
    - "**Event Data**" refers to the use of 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. 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 stored 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 in order to populate the credentials, for example – but it is reported and logged anonymously and cannot be associated with individuals in order to maintain their privacy. Behavioral Data is owned by Dashlane.

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 our Services by aggregating Usage Data (e.g., number of users within a particular jurisdiction, most popular features). This "**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 Services.

d. *Data obtained from Third Parties.* We receive information about users from our Service Providers (such as when validating an Account with a payment processor), from other users (when you are invited to try the Services) including the administrators of B2B Accounts, from publicly available sources like social media accounts, and from data providers such as marketing partners and researchers, where they are legally allowed to share this Information with us.

4. HOW DOES DASHLANE USE YOUR PERSONAL DATA?

Summary:
We use Personal Data to validate your Account, provide the Services, provide user support, communicate with you, and coordinate marketing efforts. We do not perform any automated decision making or profiling with your 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 choose not to receive 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 customer support inquiries and other requests.
- Promote the Services or send you other Dashlane marketing information, including announcements about offerings from selected Dashlane partners. Certain users, including those in Europe and Britain, must opt-in to receive marketing communications when creating an Account or afterwards. Users elsewhere (and those in Europe and Britain who have previously opted in) may always elect to stop receiving such communications.
- Manage advertising efforts on third party sites and platforms as further described below.

b. *Automated Decision Making and Profiling*. We do not use your 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 all applicable laws (e.g., GDPR) and who only have access to the data they need to provide the relevant Services. The Services will share Secured Data (which may include Personal Data) with others as you direct. We share hashed, encrypted user emails and device ids with advertisers to refine advertising efforts (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 B2B Account Administrators can access certain Personal Data and Event Data about the users of that Plan. 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 Sections 2(b) and 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. The Services will share Secured Data (which may include Personal Data) with third parties as instructed by you (e.g., when using the Services' "sharing" feature). 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 customer support, process payments, or enable communication between you and Dashlane (for example, Personal Data related to customer support requests is available to our agents on Zendesk). We review the security and data privacy practices of these 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.
- 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 subject to the GDPR. To offer the levels of protection required by European law, we have Data Processing Addenda or equivalent documents in place among our EU and US Affiliates, in addition to the other measures indicated below. Our US Affiliates are also Privacy Shield certified. See Section 10 for additional information.
- Dashlane B2B Administrators. Administrators of Dashlane B2B Accounts can see the email addresses used to access their Account and certain Event Data, including how many credentials are stored by individual users (but not which ones), password scores, and whether a password has been re-used (but not the sites on which the passwords were re-used or the password itself).
- Corporate Restructuring. If Dashlane or its business or assets are acquired by, or merged into, another company, that company will possess any Personal Data we hold at such time, 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 technically unable to provide any information about users beyond Registration Data and Event Data even if we are subject to a valid order. To the extent permitted by law, we will inform you 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 European, British, and other relevant regulations 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 re-assess 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 at, 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 will take the steps described in this Policy, including Sections 5 and 10, which are designed to ensure that all Personal Data we or our service providers process (regardless of where it originates) is secured as required by applicable laws. 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 and no longer wish to do so, you may unsubscribe from within 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. Removing your Apps does not delete your Account. To do that, see the instructions here.

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 "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. Note that unsubscribing from marketing communications will not affect operational and transactional communications, including breach notices and other alerts from within 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. YOUR RIGHTS REGARDING PERSONAL DATA (USERS IN THE EU, UK, BRAZIL, CALIFORNIA, AND NEVADA)

Summary:
*Users subject to the laws of the EU, Britain, Brazil, California, and Nevada 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 within 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. You have the following rights with respect to your Personal Data that we process. Except where indicated, these rights apply equally to users subject to the GDPR (and related laws), CCPA, and LGPD:

- 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 the Personal Data we hold about you is no longer relevant or accurate, you can request that we erase your Personal Data. If you delete your account, all Personal Data will be erased within a week of the date of deletion.
- Portability: You may request a copy of your Personal Data and may always move it to other entities as you desire.
- No Sale of Personal Data (California and Nevada Users): Go to the Do Not Sell My Personal Information page to stop all "sale" of your Personal Data. See Section 2(b) above for more information about how this works. Of course, any user can do this, regardless of jurisdiction.

b. If you wish 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 need assistance, contact the help center, email support@dashlane.com, or write us at the address below. In your request, please make clear: (i) **what** Personal Data is concerned; and (ii) **which of the above rights** you would like to enforce. For your protection, we may only fulfil requests with respect to the Personal Data associated with the email address you send your request from, and we will need to verify your identity before doing so. We will comply with your request promptly, but in any event within the legally mandated timeframes (thirty (30) days for the GDPR and forty-five (45) days for the CCPA). We may need to retain certain information for recordkeeping purposes or to complete transactions that you began prior to requesting such change or deletion.

c. We do not and will not discriminate against any user (such as by providing worse Services, 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 processing practices, or if you want to report any security violations, please contact our help center, email support@dashlane.com, or write the address below:

Dashlane, Inc.
Attn: Legal
44 West 18th Street., 4th Fl.
New York, NY 10011

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.

10. PRIVACY SHIELD

Summary:
Dashlane has self-certified with the U.S. Department of Commerce that we comply with the EU-U.S. and Swiss-U.S. Privacy Shield Principles, which provide for certain protections regarding Personal Data of citizens of these jurisdictions. While the Privacy Shield was invalidated by the EU in July of 2020, we are maintaining our certification for now.

Note: While the Privacy Shield was invalidated in July of 2020 by the European Union, we have decided to keep the certification to demonstrate our ongoing commitment to its principles and in case the program is re-instated in the future, as some expect. To ensure ongoing compliance with the GDPR, we have updated our Data Processing Addendum for B2B customers to include a valid transfer mechanism under the GDPR (the model clauses) in lieu of the Privacy Shield. In addition, because our servers are in the EU (Ireland), the U.S. government has no jurisdiction over data about non-U.S. citizens on the servers.

a. Dashlane complies with the EU-U.S. and the Swiss-U.S. Privacy Shield Frameworks established by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Data transferred from the EU and the United Kingdom and Switzerland to the United States. We have certified to the Department of Commerce that we adhere to the Privacy Shield Principles (as defined by the Department of Commerce). If there is any conflict between the terms in this Policy and the Privacy Shield Principles, the Privacy Shield Principles will take precedence. To learn more about the Privacy Shield program, the Privacy Shield Principles and to view our certification, please visit www.privacyshield.gov.

b. Our certification of compliance with the Privacy Shield Principles applies to both the Personal Data of our users and the Personal Data of our past and present employees collected in connection with their employment ("**HR Data**"). Dashlane commits to cooperate with the panel established by the EU data protection authorities ("**DPAs**") and comply with the advice given by the panel regarding HR Data transferred from the EU in the context of the employment relationship. A list of DPA contacts is available here.

c. As described in the Privacy Shield Principles, Dashlane is responsible for Personal Data that it receives and subsequently transfers to third parties. If third parties that process Personal Data for us do so in a manner that does not comply with the Privacy Shield Principles, we are responsible for such failure, unless we prove that we are not responsible for the event giving rise to the damage.

d. In compliance with the Privacy Shield Principles, Dashlane commits to resolve complaints about our collection or use of your Personal Data. EU or Swiss individuals with inquiries or complaints regarding this Policy should first contact our help center.

e. Dashlane has further committed to refer unresolved Privacy Shield complaints to JAMS, an alternative dispute resolution provider located in the United States. If you do not receive timely acknowledgment of your complaint from us, or if we have not resolved your complaint, please contact or visit www.jamsadr.com/eu-us-privacy-shield for more information or to file a complaint. JAMS' services are provided at no cost to you.

f. As further explained in the Privacy Shield Principles, binding arbitration before a Privacy Shield Panel will also be made available to you in order to address residual complaints not resolved by any other means. Dashlane is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission.