

LastPass VPN Supplemental Privacy Notice

Last Updated on October 6, 2026

Scope Of This Supplemental Privacy Notice

This LastPass VPN Supplemental Privacy Notice (“VPN Privacy Notice”) applies to your use of the LastPass VPN [solutions](#) (“LastPass VPN”) and supplements the LastPass Global Privacy Notice, which continues to govern data collected by LastPass. Where the LastPass Global Privacy Notice and this VPN Privacy Notice address the same subject matter, this VPN Privacy Notice takes precedence for data processed in connection with the LastPass VPN.

LastPass utilizes a third-party service provider to operate the virtual private network (“VPN”) infrastructure and deliver the LastPass VPN service. To provision your LastPass VPN account, we share a unique identifier derived from your LastPass account and subscription metadata with the VPN service provider. We do not share your name or email address with the VPN service provider. This is by design to enhance user privacy.

What Personal Data Do We Collect and Do Not Collect in Connection with the Use of LastPass VPN

At LastPass, we strive to limit the types and categories of personal data collected in connection with LastPass VPN to only what is necessary to provide and maintain the service. The following describes the personal data we do and do not collect:

What We Do Not Collect

LastPass VPN has been designed with a strict no-log policy with respect to your activity inside the VPN tunnel. This means that LastPass does not log, and cannot provide, records of the websites you visit, the content you access, or any other activity conducted through the LastPass VPN connection.

LastPass VPN **does not** collect the following:

- **Browsing activity and Session content.** We do not record which websites you visit, what files you download, or what content you access while using LastPass VPN. Your encrypted VPN traffic is never examined, logged, or stored.
- **DNS queries.** DNS requests sent through the VPN tunnel are not recorded.
- **IP address.** Your originating IP address is temporarily collected to establish your VPN connection. The VPN service provider then immediately encrypts this data and deletes it at the end of your VPN session. When you use the LastPass VPN, your IP address appears as one from the VPN service provider's servers (known as an "exit IP address"), which is not associated with your originating IP address. This means we are unable to connect any browsing activity to a specific user.

Data We Collect Directly From You

- **Customer Account and Subscription Data.** When you subscribe to and use LastPass VPN, we collect subscription-related metadata such as purchase time, expiration time, subscription length, trial length, plan name, and unique identifier derived from your LastPass account in order to manage your subscription and validate your entitlement to the LastPass VPN service. Your email address is used in connection with your underlying LastPass account but is not shared with the VPN service provider.

Data Automatically Collected When Using LastPass VPN

- **Device Data.** When you use LastPass VPN, we collect certain data about your device to provision and support your VPN access. This includes a device model information, operating system and a list of hashed device IDs provisioned to your account.

Data We Collect With Your Consent

- **Usage Analytics.** With your prior consent, LastPass VPN may collect analytics data to measure usage within the LastPass VPN application and to identify potential improvements. Analytics data includes a random ID assigned when you install the application, application name and version, device ID and operating system version, locale, and network type. This does not capture your VPN session content, browsing activity, DNS queries, or VPN traffic at any time, and this service does not track your activity across other applications. You may change your preference at any time from within the application settings.