NordPass Business Privacy Notice

Effective from: November 3, 2022

The General Privacy Policy describes the privacy practices of Nord's Business Services, applications, and Websites, which also apply to the NordPass Business product. Nevertheless, the provision of Services related to NordPass Business ("**NordPass Business Services**") also involves the processing of additional personal data. Please read more information below.

1. GENERAL REMARKS

NordPass Business has no technical means to access your encrypted passwords, secure notes, or other items stored in your vaults (where the End User's items are stored; "**Vault**") because we built NordPass Business based on zero-knowledge architecture. Zero-knowledge architecture means that we do not have any access to what is stored in the Vault. In cryptography, it refers to being able to prove something you know without revealing what that is. As such, our zero-knowledge password manager keeps the proof that you have the key, but not the key itself, making it very safe. No one else can see the organization's passwords, credit card details, or notes. We also don't have the organization's End Users Master Password, so the encrypted data will stay secure even if someone breaches our servers.

To understand more about NordPass Business specifications and technical features please check NordPass Business Whitepaper.

2. ADDITIONAL NOTICE TO END USERS WHEN USING NORDPASS BUSINESS SERVICES

When the End Users use NordPass Business Services with the Vault provided by an organization (our Customer), that organization can:

- Control and administer the End Users' Vault, including controlling privacy-related settings and/or features.
- Access and process End Users' personal data, including the interaction data, diagnostic data, and the contents of End Users' communications with us.
- See when End Users accessed the application, and how they used the items within the Vault (e.g., shared with others, auto-filled, deleted, etc.).
- See other available information, such as the End User's email, timestamp, item name (available only to owners, as it is specified in the NordPass Business Whitepaper), receivers of items (where applicable), etc.
- See if End Users have been breached (this info is also available for End Users; see more in Section "Data Breach Scanner").
- View End Users' password health stats (without details of items themselves) and see how many old/weak/reused passwords the End User has stored in his Vault.
- Reassign the End User's items to another End User, after the End User's Vault is deleted. All items within that Vault will be inherited by another End User to whom the Vault is reassigned.

- Delete all items in the End User’s Vault at its own discretion.

Every item in the NordPass Business Vault has two types of data: metadata (title, website address, cardholder name, etc.) and secret data (login credentials, items (e.g., passwords, notes’ content, credit card number, comments, etc.). The organization cannot see secret data. However, the End Users items, stored in the Vault, are accessible by the organization via indirect ways, e.g., through activity logs, after deletion of the End Users account, etc. Therefore, please note that the NordPass Business Vault should only be used to store items related to the organization and we highly recommend End Users not to keep any personal information there or to delete such personal information before leaving the organization/ceasing to use the NordPass Business Services.

If the End User is invited to join the NordPass Business account administered by an organization and the End User already has one’s own personal NordPass account registered with the same email address, the End User's items will be transferred to the organization which will become the controller of this data as foreseen by the applicable legal acts. In case the End User does not want one’s personal items to be transferred to the organization (to which NordPass Business account the End User is joining), we strongly advise deleting or exporting all items and adding them to another personal NordPass account (i.e. NordPass version for non-business users) created with another email address before accepting the invite to join the organization on NordPass Business.

3. NORDPASS BUSINESS AS A DATA CONTROLLER

In addition to the information provided in the General Privacy Policy, we process the following data as a data controller when you use NordPass Business Services or visit our Website:

- **Application diagnostics.** This aggregated and anonymized data helps us identify problems related to our app performance and updates. The collected information includes crash error reports and visited web addresses.

- **Anonymized app usage statistics.** We collect statistical information about the users’ activity when using NordPass Business Services: (i) the number of items stored, (ii) the date when the item was created, (iii) how the password was created (e.g., imported, autosaved, created manually), (iv) the strength of passwords in percentage (e.g., 85% of your passwords are very strong), (v) the strength of the Master Password, (vi) the percentage of suggested passwords used, and (vii) the number of different folders in the Vault. This analytical data gives us information on how our application is being used so that we can improve the NordPass Business users’ experience and the app itself.

- **Live chat widget.** If you contact us via the live chat widget, in addition to processing your contact information, we will also process your device information (such as the type of the operating system and browser) and IP address. This information is necessary for our support to determine the user’s country, prevent abuse, see if the user is connected to our servers, and help our support to process queries faster.

- **Device information.** As in the case of when you visit our Website http://www.nordpass.com/business-password-manager, we collect some device information on our application too. Such information is logged automatically and may include your IP address, browser type, operating system version, and similar non-identifying information. We may use this information to monitor, develop, and analyze the use of NordPass Business Services.

- Also, we process your photo if you provide it on a voluntary basis by uploading it to your NordPass Business account. Please note that the photo uploaded to your account will be available to other users of NordPass Business Service with whom you share and/or who share the items with you.

4. DATA BREACH SCANNER

NordPass Business offers an additional feature — Data Breach Scanner ("**Scanner**"). This feature enables scanning if certain data has appeared in any personal data breaches detected by our third-party service provider. Using a third-party provider, the Scanner checks email addresses (which were used by the End Users to join the organization) and identifies which pieces of data might be exposed. Every time you use the Scanner, you grant us permission to share your hashed email addresses with our third-party service provider. To keep your data secure, any further matching of items against the third-party's database is completed locally, on the device where it is initiated. This data will not be used by us or our service provider for any purpose other than helping to monitor data breaches where the personal data of the organization's End Users have appeared. Please note that when you use the Scanner, NordPass Business has no technical means to access your encrypted items stored in NordPass Business Vault and Scanner's search results that are shown on the users' devices.