

Privacy Policy

TREZOR Password Manager

This Privacy Policy governs above all the collection, handling and protection of your personal data by our company when using the TREZOR Password Manager Google Chrome Extension (hereinafter referred to also as the “**Trezor Password Manager**” and the “**Privacy Policy**”).

This Privacy Policy is issued to fulfill our obligations pursuant to the Articles 13 and/or 14 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to also as the „**GDPR**“ or the „**Regulation**“) to provide you with information and appropriate protection and care with regard to the processing of your personal data.

This Privacy Policy is also issued to fulfill obligations set out by the Google LLC, with its registered offices at 1600 Amphitheatre Parkway, Mountain View, California 94043, United States (hereinafter referred to also as the “**Google**”) in its Google API Services: User Data Policy of 30th May 2019.

This Privacy Policy applies to anybody, whether natural or legal person, who uses the Trezor Password Manager.

What is the Trezor Password Manager?

The Trezor Password Manager is an extension designed by us for the Google Chrome web browser. It allows you to easily store, access, manage and use your passwords. You may choose to use the Trezor Password Manager with your Dropbox user account or with your Google Drive user account depending on your choice.

The Trezor Password Manager uses Google Sign-In and Dropbox Sign-In features. By signing in, you give the Trezor Password Manager a permission to create for you a folder (“*/Apps/Trezor Password Manager*”) on your Google Drive or Dropbox to store your passwords. Each password is stored in a separate file encrypted using keys derived from your Trezor device. Therefore, you also need a Trezor device to be able to fully use the Trezor Password Manager.

You may subsequently use the Trezor Password Manager to access (and decrypt with your Trezor device) the stored passwords, to edit them, manage them and to use them to log in to respective websites and services.

Who are we?

We are a commercial company SatoshiLabs s.r.o., incorporated and existing under the laws of the Czech Republic, with its registered office at Kunderatka 2359/17a, Libeň, 180 00, Praha 8, Czech Republic, Id. No. 024 40 032, registered in the commercial register kept by the Municipal Court in Prague under file No. C 219483.

What data do we process?

The Trezor Password Manager is a self-sufficient application, that means that we **cannot and do not** collect, process or even access any of your data, personal or other, that are transmitted to the Trezor Password Manager.

However, we may at our sole discretion provide you any support necessary for you to use the Trezor Password Manager. While providing you the above-mentioned support services, we may, and occasionally will, collect and process your personal data that you choose to provide us.

Therefore, we occasionally may collect and process data voluntarily provided by you when requesting our support services such as your first and last name, your email address, your IP address including the IP address or another identifier of your device and other voluntarily provided data.

Why do we collect and process your personal data?

As mentioned above, we process your personal data to be able to provide you any requested Trezor Password Manager support services.

We collect, process and store your personal data only for the above defined purpose and only to the extent necessary to fulfill this purpose. We never conceal the purpose for which the personal data are collected and further processed.

For how long do we process your data?

We process and store your personal data only for the time necessary to meet the purpose of its processing specified above, or for the time consented by you. We comply with the mandatory rules for data archiving.

To be specific, we will process and store your personal data until the issue for which you have requested the support is solved and also for the subsequent period thereafter that is either necessary to adhere to our obligations under the applicable law, or set forth by the applicable law or in accordance therewith, or during which you or any third party may contest that we have broken any of our obligations or have violated any applicable laws in relation to the issue for which you have requested the support.

Once the purpose of the personal data processing disappears, we will destroy the personal data.

Who will have an access to your data?

We take care of your personal data security and so we choose very carefully the partners to whom we entrust your personal data.

All our partners must be able to provide sufficient security of your personal data to prevent unauthorized or accidental access thereto or other abuse thereof and all our partners must undertake a confidentiality obligation and must not use your personal data for any purpose other than the purpose for which the data were made available to them.

The recipients that may have access to your personal data are following:

- persons who provide us with the technological services or technology operators that we use to provide our services;
- persons who provide our services and websites with security and integrity and who regularly test such security and integrity;
- providers of accounting, legal and administrative services;

- our staff.

Our aim is and always will be to ensure your personal data are as anonymous as possible and unavailable to all third parties. However, under certain specifically defined conditions we will be in some circumstances required, in accordance to the applicable law, to transfer certain personal data to the public authorities.

Your personal data, no matter whether public or private, shall not be provided, alienated, exchanged, transmitted or otherwise communicated to a third party without your prior express consent unless stated otherwise herein.

How are your personal data protected?

All the personal data you provide are secured by standard procedures and technologies. We provide data protection against unauthorized or accidental access, alteration, destruction, loss, unauthorized transmission or any other unauthorized processing, as well as against any other abuse of records containing the personal data.

We are not able to guarantee the security of your personal data without your help and responsible behavior. Therefore, we ask you to help us ensure the security of your data by keeping in secret and secure the information that you provide to us when requesting the support as well as any personal data related to your use of the Trezor Password Manager by following a common security standards.

What are your rights in relation to the personal data protection?

In relation to the personal data you shall have in particular the following rights:

- a right to withdraw your consent at any time;
- a right to correct or make additions to the personal data;
- a right to request restrictions to your personal data processing;
- a right to object or complain against your personal data processing under certain circumstances;
- a right to request your personal data transfer;
- a right to access your personal data;
- a right to be informed of the personal data security breach under certain circumstances;
- a right to request a deletion of your personal data (a right to be „forgotten“) under certain circumstances; and
- other rights set forth in the Act No. 110/2019 Coll., on personal data processing (Personal Data Protection Act) and the Regulation.

Additionally, you have a right to contact the Office for Personal Data Protection in case of any violation of the obligations set forth in the Regulation with a request for remedial measures at the following address: Office for Personal Data Protection, Pplk. Sochorova 27, 170 00 Praha 7, phone number +420 234 665 111 (central telephone exchange).

Does automated decision making or profiling occur?

Your personal data are not a commodity to us. Therefore, you are not a subject to any decisions based solely on automated personal data processing and we also do not process your personal data in a way to assess certain personal aspects related to your person including analysis or estimates of your economic situation, health, personal preferences, interests, reliability, behavior, movement or your location.

Information on Google Drive user data access.

As mentioned above the Trezor Password Manager will ask you to grant it a permission to create for you a folder (“/Apps/Trezor Password Manager/”) on your Google Drive or Dropbox to store your passwords and associated information and to edit or access it during your subsequent use of Trezor Password Manager. All the information shall be stored in encrypted form. In the event you give the Trezor Password Manager your permission to access your Google Drive, this section applies to you.

The Trezor Password Manager will specifically access the information about your first and last name that you have provide to Google that will be displayed in the Trezor Password Manager when you use it.

The Trezor Password Manager will also store, access and edit the information about stored passwords and associated information including usernames and secret notes.

With reservation to your first and last name information the Trezor Password Manager will **only** access the dedicated folder that it will have created to store the passwords and associated information and to which it has been granted your previous access permission. The Trezor Password Manager will not access any other folders stored on your Google Drive to which it has not been granted access permission by you.

The Trezor Password Manager will access your Google data only to the extent necessary to provide you with the Trezor Password Manager functionality described above in this Privacy Policy, that means mainly to allow you to store your passwords and associated information in encrypted form and to access, decrypt, edit or otherwise use them (mainly to log in the third party services or websites).

How can you contact us?

If you have any questions regarding this Privacy Policy or the Trezor Password Manager in general, please, do not hesitate to contact us using the contact details below:

Contact address: Kunderatka 2359/17a, Libeň, 180 00 Prague 8, Czech Republic

Contact point (support): <https://trezor.io/support/>

Contract email address: info@satoshilabs.com

When is this Privacy Policy effective?

This Privacy Policy comes into effect on 1st December 2019. We reserve a right to amend and update this Privacy Policy at any time.

Privacy Policy
TREZOR Password Manager

Issued by SatoshiLabs s.r.o.