UPSIGNON privacy policy

Version of 07/24/2023

Data controller

- UPSIGNON, Simplified Joint Stock Company
- Head office: 121, rue Achille Viadieu, 31400 Toulouse (France)
- Registration: R.C.S. of Toulouse, n°849 484 290
- SIRET: 849 484 290 00028
- Phone: +33 6 70 743 32 99
- Data Protection Officer: Mr. Gireg Miorcec from Kerdanet
- Contact email address for processing personal data questions: privacy@upsignon.eu

Reminder of the law and the rights of UpSignOn users

UPSIGNON undertakes to respect the laws and regulations in force, in particular the Law No. 78-17 of January 6, 1978 relating to information technology, files and freedoms ("the Data Protection Act Freedoms"), and European regulation 2016/679 of April 27, 2016, entered in application on May 25, 2018, relating to the protection of physical persons with regard to the processing of personal data and the free movement of such data ("the GDPR").

The User concerned by the processing of personal data benefits from a right of opposition which can be exercised at any time by contacting the UPSIGNON Data Protection representative within the conditions defined below.
In the event that this right is exercised, the User may no longer access the features of the Application that require it.

The User also benefits from rights of access, rectification and deletion of his personal data allowing him in particular to access information concerning him and to demand that his data are, as the case may be, rectified, supplemented, updated or removed.
The User also benefits from a right to portability allowing him in particular to recover the data related to him that are processed by the company UPSIGNON for its personal use and/or to transfer it to new organisations.

Any question or request related to the processing of Personal Data should be sent electronically to: privacy@upsignon.eu The UPSIGNON has to respond within one (1) month from the date of receipt of the User's request.

In the event that the User is not satisfied with the answers of the UPSIGNON company to its claims or would consider that the processing of personal data is

against the law, he can contact the National Commission for Information and Liberties (CNIL), 3 Place de Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07, Tel. : 01 53 73 22 22, Website Web: www.cnil.fr.

UPSIGNON's commitment

Respect for your privacy is a core value of UPSIGNON.
The app and all related features are designed with the objective of limiting as much as possible the quantity of personal information that is collected and processed by UPSIGNON. We therefore apply as far as possible the principle of "Privacy by design".
In the event that processing is necessary for providing the services offered, we are committed to protecting all data which can be collected in the most secure way possible, during their transfer, as well as their storage.
UPSIGNON does not intend to transfer or sell data generated through the application to third parties. However, we reserve the right to subcontract certain technical tasks which may involve a processing of personal data to European third parties hosted in Europe.

Details of treatments

Here is the list of personal data processing carried out via the UpSignOn app.

PERSONAL vaults

Storage of your data on the UpSignOn server, in an encrypted form

When you synchronize your personal vaults across multiple devices, the data you have entered in your vault (passwords, codes, email addresses, notes, bank cards, IBANs, urls, etc.) are sent and stored on our server. Data sent to the server are encrypted with a randomly generated key which is stored only on your devices. The UpSignOn server only has access during this process to one random identifier, a random authentication code and the encrypted file.
This system is extremely secure, your data is perfectly unreadable by UPSIGNON. Furthermore, these data is not associated with identifying information (UPSIGNON does not even know your email address).
This operation allows the correct synchronization of your data between your devices as well as the backup mechanism via a trusted contact that is the only one who knows how to make the link between you and the identifier of your vault on the server.

Your vault's data is kept on the server without time limit as long as your vault remains active. It is automatically deleted after 6 months of inactivity. You can also have it deleted by requesting the deletion of your vault within the app from all your devices.

- Purpose: to make possible the synchronization and data recovery features.
- Optional processing: yes, this processing only exists from the creation of a personal vault, it is however mandatory as soon as a personal vault is created
- Legal basis for processing: legitimate interest of UPSIGNON for the purpose of providing the requested functionality
- Storage period: deletion after 6 months of inactivity on the vault
- Recipient of the data: UPSIGNON and its hosting subcontractors
- Type of data collected: all information and secrets entered by the user in the application.
- Anonymous data: yes
- Encrypted end-to-end data: yes
- Encrypted data during communications: yes

Storage of your shared vaults on the UpSignOn server, in an encrypted form

When you share secrets through the UpSignOn app, you create the equivalent of a personal vault on the UpSignOn server. This shared vault works the same way as a personal vault. Data is end-to-end encrypted with a random key that is kept by all recipients in their personal vault.
During this process, the UpSignOn server only has access to a random identifier, a random authentication code and the encrypted file.
This system is extremely secure, your data is perfectly unreadable by UPSIGNON. Furthermore, the data is not associated with identifying information (UPSIGNON does not even know your email address).
This operation allows the correct synchronization of your data between the vaults of the various recipients of the shared data.

The data of your vaults is kept on the server without time limit as long as the shared vault remains active. It is automatically deleted after 6 months of inactivity on the shared vault. You can also have it deleted by requesting the deletion of the shared vault in the application.

- Purpose: to make sharing between trusted contacts possible
- Optional processing: yes
- Legal basis for processing: legitimate interest of UPSIGNON for the purpose of providing the requested functionality
- Storage period: deletion after 6 months of inactivity of the shared vault
- Data recipient: UPSIGNON and its hosting subcontractors
- Type of data collected: all information and secrets added by the user in the shared area in the application.
- Anonymous data: yes
- Encrypted end-to-end data: yes
- Encrypted data during communications: yes

PROFESSIONAL vaults

For professional vaults, we distinguish the user from the customer. The customer takes out licenses with UPSIGNON for the use of its beneficiaries (employees, service providers) called users.

Encrypted storage of your SAAS professional vaults on the UpSignOn server PRO

SAAS pro vaults are stored on the UpSignOn PRO server. They are associated with the email address of their owner. This operating mode makes it possible to avoid having to manage trusted contacts as for personal vaults for the functionality of sharing and helps preventing data loss in the event of loss of authorized devices. Your pro vault data is encrypted by your master password and remain perfectly unreadable by the UPSIGNON company.

Your vaults data is kept on the server without limitation of duration until its owner or the UpSignOn PRO customer requests its deletion.

- Purpose: to make the pro vault functionality possible
- Optional processing: no, required to open a pro vault
- Legal basis for processing: legitimate interest of UPSIGNON for the purpose of providing the requested functionality
- Storage period: unlimited as long as the contract between UPSIGNON and the customer persists or as long as the deletion of the data is not requested by the user or the customer.
- Recipient of the data: UPSIGNON and its hosting subcontractors
- Type of data collected: user's email address, all the data entered by the user in his vault.
- Anonymous data: no
- End-to-end encrypted data: yes, excluding the vault's email address
- Encrypted data during communications: yes

Encrypted storage of shared SAAS pro vaults on the UpSignOn pro server

Shared SAAS pro vaults are stored on the UpSignOn PRO server. They are associated with the email addresses of their recipients.
Shared pro vault data is encrypted by a random key known only to recipients of the shared vault and remain perfectly unreadable by UPSIGNON.

- Purpose: to make possible the functionality of sharing data between professional vaults
- Optional processing: yes
- Legal basis for processing: legitimate interest of UPSIGNON for the purpose of providing the requested functionality
- Storage period: data retained until deleted by their manager or until the deletion of all recipient vaults

- Recipient of the data: UPSIGNON and its hosting subcontractors
- Type of data collected: email address of recipients, all the data that is entered by users in the shared vaults.
- Anonymous data: no
- End-to-end encrypted data: yes, excluding email addresses of recipients
- Encrypted data during communications: yes

Storage of shared and unshared SAAS pro vault statistics on the UpSignOn PRO server

SAAS professional vaults are supervised by the customer. The customer can thus observe the evolution of the strength of the user passwords.

- Purpose: make monitoring functionality possible
- Optional processing: no
- Legal basis for processing: legitimate interest of UPSIGNON for the purpose of providing the requested functionality
- Storage period: data kept until the deletion of the associated professional vaults
- Recipient of the data: UPSIGNON and its hosting subcontractors, the customer.
- Type of data collected: number of strong, average and weak passwords by vault, logs of connection and action performed in the application by users.
- Anonymous data: no
- Encrypted end-to-end data: no
- Encrypted data during communications: yes

Update to this policy

UPSIGNON reserves the right to update this Privacy Policy at any time and without prior notice.

Any change to this Policy will be reported in the Application.