PRIVACY POLICY - MOBILE APPS

CONTEXT

The mobile app, installed from Google Play or App Store, cannot be used without a purchased service from a Service Provider. It can only be used with an account created for you in advance. An account can never be created in the app itself. The app is therefore used to **give** access to purchased services. The content of the services may differ depending on the agreement with the Service Provider. Examples of such services are:

- Searching for contacts configured in own or federated organisation(s)
- Viewing contact's information, such as name, avatar, email address, telephone number and presence
- Making calls (GSM or mobile VoIP) to such contacts or contacts on your own device
- Establish individual chat sessions and collaborative groups (rooms). In these chats or rooms, information can be shared. This includes file sharing as well as online meetings with screen sharing and video. Participants in rooms can be internal users (organisational contacts) as well as external (invited by email). In online meetings, external users may participate after having been invited with their mobile phone number.

THIRD-PARTY DISCLOSURE

User data is never transferred, traded or disclosed to any 3rd party that is not an integrated part of the purchase service. The service may include "Collaboration" as described below, but also other services, e.g., Call Recording or integration to CRM systems. Contact your Service Provider for details.

COLLECTED DATA

The app runs in a sandbox and data in the app is not available from the outside.

The app will never collect data from the device itself, from any native personal configuration or any other apps. It is only the user of the app that based on the purchased service may collect and share data with other users. Before being able to do so, the user must give the app necessary permissions to e.g., photo library, contacts or file system.

SHARED DATA

All data in transit is encrypted using TLS (Transport Layer Security).

Collaboration

In the context of chats and collaboration (rooms), a user can deliberately share:

- Text
- Any type of files
- Voice recordings (as a message)

This data is stored on an integrated 3rd party server while the service is in use.

Shared files can at any time be deleted by the user that shared it. Shared text and voice recordings cannot be individually deleted. If the user is the owner of a collaborative room, he can at any time delete it including all collected data.

Avatars

A user can select an image from photo library or use the camera to take a photo used as profile picture (avatar). This avatar will be stored on the Service Provider's server and be visible for all internal users that are authorized to search for you as a user.

Contacts

The app never automatically collects or shares contact information from the device.

A user may add a native contact as a contact in the app. This contact's vCard will then be stored on a server provided by the Service Provider. It can however not be accessed by anyone but the user that added it.

Contacts from within the organisation of the purchased service, can be synced to the local (native) address book. The purpose with this, is to be able to find contact details also when being off-line and to make name lookups when receiving direct GSM calls from these contacts.

On Android, synced contacts are stored in a separate group inside the native contacts app. The group (including all vCard's) is automatically removed when sync is disabled, or the app is uninstalled.

On iOS, the sync is implemented by installing a profile (downloaded from the Service Provider's server) and the contacts can be synced to the device. When sync is disabled in the iOS app, the contacts will remain until the profile is deleted.

The synced contacts may also be removed if the Service Provider remove the service or alter the configuration of which type of contacts that can be synced.

Crash reports

Crash reports never include data that can identify a user or person. They are entirely used for fault locating purposes by the developer. They are stored on Google and Apple servers.

Crash reports from the Android app are automatically submitted.

Crash reports from the iOS app are submitted only if the user has activated it on the device. In *Settings/Privacy/Analytics & Improvements*: enable *Share iPhone Analytics* + *Share With App Developers*.

Diagnostics

The app holds a feature to collect clear text diagnostics for fault locating purposes. This feature is by default turned off and can only be activated by the user. When diagnostics is collected, it stays inside the app until the user decides to share it. It can only be shared by the means of sending an email to a receiver decided by the user. The user may therefore be able to fully inspect the content before it is shared with someone else.

REMOVAL OF DATA

As the main purpose with the app is to give access to a purchased (preconfigured) service, the app does not offer a way to remove your account and data connected to you as a person. To do that, contact the Service Provider where the service was purchased.

When the app is uninstalled from the device, all local data is automatically deleted. But shared data as described above, will remain until the account is removed.