KOMPAAS.TECH GMBH

SoftPhone & WebPhone Privacy Policy

Introduction

This Privacy Policy explains how KOMPaaS.tech GmbH (hereinafter referred to as the Operator) processes personal data when you use the KOMPaaS communication applications for mobile devices and web browsers (hereinafter — the Apps).

It supplements and forms part of the Operator's documents published on the Operator's Website:

- Communication Service Offer;
- Agreement on usage of MyKOMPaaS Account;
- Data Privacy Statement (GDPR, EU).

Last updated: 26 October 2026. Version 1.0.

Terms

Term	Definition
Operator	KOMPaaS.tech GmbH, Lindengasse 56, 1070 Vienna, Austria, Commercial Register FN 461303 m, acting as data controller within the meaning of Art. 4(7) GDPR.
Apps	The KOMPaaS communication applications: the mobile application for Android and iOS (KOMPaaS SoftPhone) and the browser extension for Chrome, Firefox, Safari and Opera (KOMPaaS WebPhone), provided by the Operator for voice and video calls via SIP/WebRTC and for messaging.
Subscriber	An individual person, individual entrepreneur or legal entity that has joined the Communication Service Offer and whose Services are accessed through the Apps.
User	A natural person who uses the Apps with credentials issued under a Subscriber's MyKOMPaaS Account, including employees and authorised representatives of the Subscriber.
Personal data	Any information relating to an identified or identifiable natural person, as defined in Art. 4(1) GDPR.
Traffic data	Data generated when the Apps are used to make or receive calls, including calling and called numbers, date, time, duration, direction and status of calls, and IP addresses.
Call recording	The function of the Virtual PBX Service that, when enabled by the Subscriber, stores the audio of calls in the Subscriber's disk space.

Term	Definition
Installation identifier	A technical identifier generated for the specific installation of the App on a device (ANDROID_ID on Android, identifierForVendor on iOS), used to distinguish devices for session and notification management.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).
TKG	Austrian Telecommunications Act 2021 (Telekommunikationsgesetz 2021).

1. Scope and roles

1.1 This Privacy Policy applies to the processing of personal data in connection with the installation and use of the Apps on the User's device or browser and the related processing on the Operator's communication network.

1.2 The Apps are SIP/WebRTC clients intended for business use. They enable Subscribers and their Users to make and receive voice and video calls through Subscriber numbers and Virtual PBX Services, to exchange messages, and to manage their Services under the Communication Service Offer.

1.3 Where a User uses the Apps on behalf of a Subscriber, the Subscriber determines the business purposes of the communications and acts as controller for that processing. The Operator acts as a provider of communication services and, in respect of data stored on the Subscriber's instructions (such as Call recordings and PBX statistics), as a processor within the meaning of Art. 28 GDPR.

1.4 Processing of personal data on the Operator's Website, in the MyKOMPaaS Account, for identification of Subscribers and for billing is described in the Data Privacy Statement published on the Operator's Website.

2. Personal data processed

2.1 Depending on how the Apps are used, the Operator processes the following categories of personal data:

Category	Data	Source
Account and authentication data	Login (phone number or e-mail address), one-time codes, two-factor authentication codes, session tokens, MyKOMPaaS Account and Subscriber identifiers, assigned extensions and Subscriber numbers. SIP credentials are issued by the Operator's server after login and are not entered by the User.	Entered by the User; issued by the Operator.
Traffic data	Calling and called numbers, date, time, duration, direction and status of calls, outgoing number selected, IP address.	Generated when calls are made or received.

Category	Data	Source
Call and message content	The audio and video of calls, transmitted in real time to establish the Connection, and the content of messages exchanged through the messaging function. Call audio is stored only where the Subscriber has enabled Call recording or transcription Services.	Microphone and camera of the User's device; entered by the User.
Contacts	Names and phone numbers from the device address book (read-only access), only where the User grants the corresponding permission.	Device address book (optional).
Device and technical data	Device model, operating system version, App version, Installation identifier, push notification token, network state, diagnostic logs.	Collected automatically by the App.
Support data	Content of support requests and related correspondence.	Provided by the User or Subscriber.

2.2 The mobile App requests the following device permissions: microphone (voice calls), camera (video calls and login by QR code), contacts (read-only, to display the address book), notifications and full-screen notification for incoming calls, Bluetooth (headsets), vibration, network state, and foreground or background operation required to maintain the SIP registration, keep calls active and synchronise messages. The browser extension requests permissions for notifications, local storage, background operation, push messaging and access to the Operator's service domains; microphone and camera access is requested only when a call is started.

2.3 The Apps do not request access to location, phone state, call log, SMS, device storage or write access to contacts. The Apps do not collect the IMEI, advertising identifiers (IDFA / Advertising ID) or any other identifier intended for advertising or cross-app tracking.

2.4 The Operator does not process special categories of personal data within the meaning of Art. 9 GDPR through the Apps.

2.5 The Apps do not contain analytics or advertising software development kits. The Operator does not sell personal data and does not use personal data obtained through the Apps for advertising purposes or share it with advertising networks.

3. Purposes and legal bases

3.1 The Operator processes personal data for the following purposes and on the following legal bases:

Purpose	Data	Legal basis

Purpose	Data	Legal basis
Provision of the Services: authentication, registration of the App on the Operator's network, establishing, holding and transferring voice and video calls, delivery of messages and incoming-call notifications	Account data, traffic data, call and message content (transmission), device data	Performance of the Agreement, Art. 6(1)(b) GDPR
Billing and call statistics in the MyKOMPaaS Account and Virtual PBX	Traffic data	Art. 6(1)(b) GDPR; legal obligations under Austrian tax and commercial law, Art. 6(1)(c) GDPR
Call recording and transcription, where enabled by the Subscriber	Call content, traffic data	Processing on the Subscriber's documented instructions, Art. 28 GDPR
Network security, detection and prevention of fraud and abuse, resolution of failures	Traffic data, IP address, device data, logs	Legitimate interests of the Operator in the integrity and security of its network, Art. 6(1)(f) GDPR; § 167 TKG
Display of the device address book in the App	Contacts	Consent of the User, Art. 6(1)(a) GDPR, given through the device permission
Support and troubleshooting	Support data, device data, logs, relevant traffic data	Art. 6(1)(b) and Art. 6(1)(f) GDPR
Compliance with legal obligations, including lawful requests of courts and authorities	Data required by the request	Art. 6(1)(c) GDPR; TKG

3.2 For the purpose of fraud prevention and network security, only traffic data (e.g. frequency, duration and destination of calls) is analysed. The content of communications remains confidential unless otherwise required by law.

3.3 The Subscriber is responsible for the lawfulness of Call recording, including informing the participants of a call and, where required, obtaining their consent.

3.4 The Operator does not use personal data obtained through the Apps for profiling or for automated decision-making that produces legal or similarly significant effects on the User.

4. Recipients and transfers

4.1 The Operator discloses personal data only to the extent necessary for the purposes set out in Section 3, to the following categories of recipients:

- the Subscriber under whose MyKOMPaaS Account the User is registered: traffic data, statistics and, where enabled, Call recordings are available to the Subscriber's administrators;
- telecommunications operators with whose networks the Operator interconnects, to the extent required to route and complete calls;

- push notification services operated by Google (Firebase Cloud Messaging) and Apple (Apple Push Notification service), which receive the push token and the information needed to deliver incoming-call and message notifications to the User's device;
- STUN servers operated by Google (stun.l.google.com), which the App contacts when establishing a call in order to determine the public network address of the device; only the IP address and port are disclosed, and no call content passes through these servers;
- service providers hosting the Operator's infrastructure or providing technical support, acting as processors under data processing agreements in accordance with Art. 28 GDPR;
- courts, public authorities and regulators, where the Operator is legally obliged to disclose data.

4.2 Personal data is processed in Austria and in other member states of the European Union and the European Economic Area.

4.3 Where personal data is transferred to a country outside the EU/EEA (in particular to Google and Apple for push notifications and STUN), the Operator ensures an adequate level of protection by means of an adequacy decision of the European Commission, including the EU–US Data Privacy Framework, or appropriate safeguards such as the EU Standard Contractual Clauses (Art. 44 et seq. GDPR). A copy of the applicable safeguards may be requested from the Operator.

5. Retention periods

5.1 The Operator retains personal data only for as long as necessary for the purposes for which it was collected, or as required by law:

Data	Retention period
Account and authentication data	For the term of the Agreement. After termination, Subscriber and User data is archived for 90 days and then permanently deleted.
Traffic data used for billing	Until the invoice is settled and the period for disputing it has expired, or until a pending dispute is finally resolved. Billing records are retained for 7 years under § 132 BAO and § 212 UGB.
Call recordings and transcripts	For as long as the Subscriber keeps them in the Subscriber's disk space. The Subscriber may delete them at any time. Deleted together with the Subscriber's data after termination.
Call content not recorded	Not stored; transmitted in real time only.
Messages	For as long as the Subscriber's messaging Service is active, unless deleted earlier by the User or the Subscriber. Deleted together with the Subscriber's data after termination.
Contacts	Not stored by the Operator; read from the device address book only while the App is in use.
Push tokens, Installation identifier, device data	Until the User logs out of the App, uninstalls it, or the data is replaced.

Data	Retention period
Diagnostic and security logs	For a limited period necessary to ensure the security and stability of the Services.
Support data	3 years after the request is closed.

5.2 Where data must be retained beyond these periods under a legal obligation, its processing is restricted to that purpose. Data may be anonymised instead of deleted.

6. Security

6.1 The Operator applies appropriate technical and organisational measures to protect personal data against unauthorised access, loss, alteration and disclosure.

6.2 All communication between the Apps and the Operator's network is encrypted in transit: HTTPS for application traffic, SIP over secure WebSocket (WSS) for signalling, and DTLS-SRTP for voice and video media.

6.3 The User's password is not stored on the device. Session data on Android is encrypted with AES-256-GCM using a key held in the Android Keystore; on iOS it is stored in the Keychain restricted to the device and excluded from iCloud and backups. SIP credentials are stored in encrypted form. Messaging tokens are held in memory only. Local data such as the call log and message cache is protected by the operating system's application sandbox.

6.4 Access to stored traffic data and Call recordings is restricted to the Subscriber's authorised Users and to the Operator's personnel who require such access to provide the Services, all of whom are bound by confidentiality obligations.

7. Rights of the data subject

7.1 Under the GDPR, the User has the right to:

- request information about the personal data processed, the purposes, recipients and retention period (Art. 15 GDPR);
- request rectification of inaccurate or completion of incomplete data (Art. 16 GDPR);
- request erasure of data where it is no longer necessary, unlawfully processed, or where consent has been withdrawn or an objection has been raised (Art. 17 GDPR);
- request restriction of processing (Art. 18 GDPR);
- receive the data provided to the Operator in a structured, commonly used and machine-readable format, such as CSV (Art. 20 GDPR);
- object to processing based on legitimate interests on grounds relating to the User's particular situation (Art. 21 GDPR);
- withdraw consent at any time with effect for the future (Art. 7(3) GDPR), for example by revoking the contacts, microphone or camera permission in the device settings;
- lodge a complaint with the Austrian Data Protection Authority (Datenschutzbehörde, Barichgasse 40–42, 1030 Vienna, www.dsb.gv.at) or with the supervisory authority of the User's place of residence.

7.2 Requests may be addressed to the Operator at privacy@kompaas.tech or by post to the address indicated in Section 10. The Operator responds within one month.

7.3 Where the User uses the Apps under a Subscriber's MyKOMPaaS Account, the Operator may forward the request to the Subscriber as controller or ask the User to contact the Subscriber directly.

8. Deletion of account and data

8.1 Logging out of the App removes the User's session data and SIP credentials from the device and clears the local call log and message cache. Uninstalling the App or removing the browser extension removes all data stored locally by the App.

8.2 User accounts within the Apps are managed by the Subscriber. A User may request deletion of the account from the Subscriber's administrator in the MyKOMPaaS Account or Virtual PBX, or by sending a request to privacy@kompaas.tech stating the login and the name of the Subscriber.

8.3 Upon deletion of a User account, the authentication data and, after the archive period specified in Section 5, all associated traffic data, messages and Call recordings are deleted, except for data the Operator is required to retain by law.

9. Children and changes to this Policy

9.1 The Apps are business tools and are not intended for persons under the age of 16. The Operator does not knowingly process personal data of children.

9.2 The Operator may amend this Privacy Policy to reflect changes in the Apps, in processing activities or in applicable law. The current version is published on the Operator's Website at https://kompaas.tech/softphone-privacy/. Material changes are communicated through the Apps or to the Subscriber by e-mail.

10. Contact

KOMPaaS.tech GmbH

Lindengasse 56, 1070 Vienna, Austria

Commercial Register: FN 461303 m

E-mail: privacy@kompaas.tech

Phone: +43 1 412 00 99