Privacy Factsheet for Avaya Workplace Application

Version: May 2021

Some Privacy Facts about Avaya Workplace:

- *Workplace is a software client. This means, the details of data processing depend on the underlying core solution(s) that drive the used services. Please reach out to the administrator of your core system to find out more about the concrete data processing.*
- *Workplace only processes personal data it needs to provide you with certain functionalities.*
- *Besides the data processing in the core solution(s), Workplace itself does not share any data with Avaya or other third parties, except for aggregated and anonymized technical data for the sole purpose of quality improvement of Workplace.*
- *There is only a limited amount of personal data stored within Workplace itself on your local device. The application enables you to access your data from the designated network each time you start Workplace.*
- *Workplace includes "pre-meeting" and "in-meeting" features to empower you to make decisions regarding your and your guests' personal data being processed within the Workplace application.*

Avaya Workplace ("Workplace") is a client/end-point application for Avaya communication solutions which enables you to access many features from a wide range of Avaya communications and collaboration systems from a single application. It can be used in conjunction with your Avaya desk phone or enable you to work remotely without compromise by using your supported mobile device. Depending on the capabilities of the connected core-solution, it provides you *inter alia* with key telephony features of Avaya Aura and IP Office telecommunication systems, voice & video, rich conferencing, instant messaging, presence, corporate directory access, desktop integration and remote worker support.

The processing of personal data by the underlying solution(s) may vary and is not covered in this privacy factsheet. For more information regarding the underlying Avaya solution(s), please reach out to the administrator of the core system(s) or services you're accessing with Workplace.This document provides general information on how Workplace processes your personal data and describes the privacy features embedded within Workplace.

In the context of this document, *"host"* means someone who can host meetings; *"you"* or *"user"* or *"participant"* means the individual using Workplace; "*member*" means an individual who has been invited into the meeting and has been given certain data access privileges by the host.

1. Who is providing Avaya Workplace?

Workplace is software from Avaya. Click here for more information on Avaya.

2. What types of personal data might be processed by Workplace and for what purposes?

Workplace only processes personal data necessary to provide you with its functionalities. Below is a list of the personal data categories (along with specific data usage purposes) that, depending on the concrete use case, may be processed by Workplace.

Personal data collected directly from you:

Type of Data	Examples	Workplace uses it to…
Identifiers	Your first and last name, email address (username), phone number	Locate your account(s) and services Respond to support requests Communicate to/with you To provide associated application services and features
Other account-related data	Account credentials, language settings, and personal preferences (e.g., auto-start/login, auto set to away, etc.).	Login to your account(s) To provide associated application services and features
User-provided content (i.e., data you or others upload or create while using Workplace)	Public/private chat and attachments, recorded (welcome) greetings, mailbox greetings, meeting recordings, contacts and favorites, create and join scheduled meetings, and any other information you share while using Workplace	Store chat records and files (so you may refer to them later) Store meeting recordings (which may contain audio, video, and screen sharing elements) Store contacts and favorites to reach your business contacts quickly Join, create, and schedule meetings and conferences

Personal data generated by Workplace:

Type of Data	Examples	Avaya Workplace uses it to…
Technical information related to your device(s), browser, Workplace app, internet connection and network	Call history, meeting history, IP address, browser type, Workplace platform (iOS, Android, MacOS, Windows) and Workplace app version, type of camera, microphone or speakers, connection type, scheduled meetings and conferences, etc.	Store call, meeting history records, so you may call, text, email the person back. Provide associated Workplace services and features Respond to support requests Monitor performance of our data centers and networks Improve Workplace through anonymized and aggregated data

Settings and preferences chosen by you	Auto-start preference Presence preference Application integration (Google Chrome click to dial browser extension, Outlook-add on, Headset controls) Keyboard shortcuts Contact preferences Display settings (language) Video calls on/off Join meeting with video on/off Join meeting with audio on/off Require meeting password Narrator on/off Enable/disable notifications Choose an "other phone" for your business calls Messaging (emojis, animation, spell check) preferences	Tailor your experience with Workplace
Metadata	Time and duration of the call, and call participants Time of each instant message sent, and the messaging participants Time of the meeting, and meeting participants Join and leave time of participants Email address, name, (display name) or other information that a participant enters to identify themselves in the meeting	To provide associated application services and features Respond to support requests

3. Avaya does not access your content within Workplace.

Workplace data (including recordings, instant messages, call history, your contacts) belong to you and the organization responsible for the underlying solutions(s). Avaya does not access your content data on Workplace, unless Avaya is instructed (by your organization) to provide technical support.

Avaya may collect via Workplace aggregated and anonymized technical data (i.e., data that does not directly identify a human being) regarding how the use of Workplace, such as how frequently Workplace is utilised, how many calls/conferences are made, how many instant messages were sent/received, etc. for the sole purpose of improving Workplace. Administrators can disable such collection for its users on a corporate account level, or you can deactivate this feature yourself in the settings of Workplace.

4. Privacy features within Workplace.

Workplace has a variety of features (so-called *"privacy by design and default"* features), which will empower you to make decisions regarding the use of your personal data. Depending on the Workplace configuration set by your organization (i.e., our Customer), some features or settings may not be visible to you.

- Authentication

  Workplace supports several authentication methods (e.g., Username/Password, Unified Login, Avaya Authorization, Avaya Cloud Authorization, Microsoft Modern Auth, Integrated Windows Authentication) to secure your data and assert your identity. Workplace will securely store your passwords in the platform security manager of your selected device or workstation. For additional security, you may choose to enter your passwords each time you launch Workplace.

- Call history

  Call history records may be deleted at any time from the history pane of the Workplace application.

- Contacts and favorites

  You may choose to allow Workplace to load only your corporate contacts or (in addition) your other contacts available on the device where Workplace is installed. Also, you may choose to select the contacts to appear in the list of "favorites".

- Desktop / Application / Whiteboard sharing

  During presentation mode, you may choose what to share with other participants: (i) entire screen, (ii) portion of the screen, (iii) application(s), (iv) whiteboard.

- Set timing for the meeting

  The host may set the timing for the meeting which will result in a notification being played to the participants before the meeting ends (unless the host will take an action to extend the meeting).

- Controlling meeting participants

  The host may:

  - Audio mute/unmute the audio feed of any participant;
  - Block/unblock the video feed on any participant;
  - Remove a participant from the meeting;
  - Lock the meeting to prevent the admission of unauthorized (or late) participants;
  - Provide a one-time pin for the meeting.

- Meeting recordings

  Workplace enables hosts to create audio and video recordings of meetings. Workplace will alert all participants via both audio and video that the meeting is being recorded. The designated participant, member(s) and/or other parties (to be chosen by the host) may access/download the recorded meeting to

his/her local storage device or keep it on the conference server. Recording permissions can be managed from the web-based meeting portal, accessible from Workplace.

- Conference chat

  Workplace allows you to archive conference chat to a local file.

- Camera and microphone

  Workplace allows you to automatically block your camera and microphone each time you enter the meeting.

- Controlling who may see your presence

  Workplace allows you to manage your presence watchers (who you allow to observe your presence).

- Instant messaging conversation

  Messaging participants may:

  - Remove a participant from a conversation;
  - Leave the conversation;
  - Archive conversation contents to local file(s).

- Deleting your Workplace data within the application

  Workplace offers a "reset application" option, which will remove your Workplace data (i.e., logs, local settings, account credentials) from your device or workstation. After resetting the Workplace application, Workplace must be reconfigured before it can be used. This will not affect your other Workplace data (e.g., recordings, contacts, call history, etc.) being stored on the network.

- Calendar data

  Workplace allows you to choose what calendar(s) to load (in a read-only mode) into the application to enable through one-click to join meetings.

- Voice mail

  Workplace offers voicemail box message waiting indicator and one-click dial to access your voicemail box.

5. How long is your content is being kept within Workplace?

The administrator of the underlying solution(s) can determine the retention period for all content (e.g., files, direct messages, recordings, etc.) stored within Workplace on your device. Apart from that, you have various data retention controls within your Workplace:

- Call history items may be deleted by you from within Workplace at any time;
- Contact data may be deleted by you from within Workplace at any time;
- Calendar data is downloaded from your calendar provider at runtime. If you delete any calendar items in your calendar application, they will be removed from Workplace;
- Instant messaging data is downloaded from the messaging service at a runtime. Your organization may opt-in to allow you to archive your messaging conversation to a file;
- Conference chat may be archived locally while the conference is active. Conference chat is not available after the conference has ended;
- Diagnostic logging maintains up to approximately 100 MB of space (data to be stored on your device) and such logging data rolls over based on usage. You may minimize the diagnostic logging frequency within Workplace settings, however, in the event you choose to report a technical issue you are experiencing within Workplace to your organization, limited amount of logs might not provide the required technical details to fix an issue.

- END OF THE PRIVACY FACTSHEET -