Privacy Statement for Avaya Mobile Identity

Version: January 2020

We have prepared this privacy statement *("Privacy Statement")* to disclose how Avaya Inc. (4655 Great America Parkway, Santa Clara, CA 95054-1233, USA) or its applicable worldwide affiliates *("Avaya" "Us" or "We")* processes your *("You," "Your" or "Yourself")* personal data (i.e., data that identifies or may be used to identify an individual) *("Personal Data")* during the provisioning of Avaya Mobile Identity Services *("AMI")*.

1. What types of Your Personal Data do We process?

Below is a list of the main Personal Data categories (along with some specific data usage purposes) (i) to be collected directly from You (e.g., name, telephone number, biometrics, email address) and/or (ii) to be generated by Avaya during the creation of Your account, including authentication sessions (e.g., IDaaS Identity ID, private encryption key, metadata), collectively Your *("Avaya Digital ID")*:

- First Name (Middle Name) and Last Name

  When the Avaya enterprise customer, which has subscribed to AMI, *("Avaya Enterprise Customer")* You interact with intends to authenticate You via AMI, We will provide Your name to such company for Your identity verification purposes.

- Telephone Number

  Your telephone number will be the primary identifier of Your Avaya Digital ID while using AMI and will be provided by Us to Avaya Enterprise Customers during subsequent authentication sessions. Also, before each authentication, except for standard voice biometric check, You will receive an SMS text message along with a hyperlink to the AMI web application to enable You to undergo the facial biometric challenge.

- Biometrics (Voice-print and Face-print)

  By using the camera and microphone on Your smart device, We will enable You to record Your face-print and voice-print to support the primary method by which AMI will attempt to authenticate You. Your biometrics (i.e., face-print and voice-print) that are already associated with Your Avaya Digital ID will then be compared against the new biometric sample(s) You provide (either during the call [voice-print] or via web application [face-print]) before each subsequent authentication. To facilitate the potential re-training of biometric models that are associated with Your Avaya Digital ID, and to compensate for the longer-term effects of aging on the biometric samples You share with Us, respective subsequent biometric samples will also be collected and stored in an encrypted format, with a separate encryption key per sample. Such a collection of biometrics will enable more precise decisions when You attempt to authenticate Yourself via AMI. Your biometrics will not be provided to Avaya Enterprise Customers with which You interact; however, We may use their existing IT infrastructure to collect Your voice-prints when You call them.

- Email Address

  It will be used as the secondary identifier of Your Avaya Digital ID to associate it with Your other device(s) (e.g., tablet). Also, it will be used in case You request to recover Your Avaya Digital ID, change Your phone number, to notify You that Your Avaya Digital ID is going to be deactivated in case You do not use it for a specific period of time referenced in Section 5 "*How long do We keep Your Personal Data?"* of this Privacy Statement, provide You with a support in case You have any questions with regards to AMI, send You newsletters / notify You with regards to the updated legal terms (e.g., terms of use and this Privacy Statement) and for other reasonable purposes allowed by applicable laws.

- IDaaS Identity ID

  A unique internal identifier will be generated and associated with Your Avaya Digital ID that will act as an additional factor of Your identity verification and authentication. Such a unique identifier will also be used to link Your Avaya Digital ID with pseudonymized Personal Data stored on the blockchain. In addition, Your IDaaS Identity ID will be communicated (at a time You make a call) to Avaya Enterprise Customers that have subscribed to AMI, to recognize that You have created Avaya Digital ID for authentication purposes.

- Private Encryption Key

  During the creation of Your Avaya Digital ID, Avaya will generate a private encryption key, to be associated with Your Avaya Digital ID, and then store such key on Your device so the next time You want to use Avaya Digital ID - We will be able to check whether You have that key before initiating an authentication session. Such a key is strictly necessary to enable Avaya to deliver AMI services. In the event You change Your initial device, You will be asked to go through a re-keying process that involves passing biometric check(s) and confirming via mail that You want to use this different device.

- Metadata

  This constitutes any technical data, included but not limited to, generated during creation of Your Avaya Digital ID (e.g., legal terms version number, date and time of acceptance, date and time of granted consents, etc.), enrollment and/or authentication attempts with respective Avaya Enterprise Customers (date and time of authentication attempt, authentication challenge IDs, requesting Avaya Enterprise Customer IDs, etc.). Such data also may be provided by Avaya to its Enterprise Customers for authentication, billing (i.e., while AMI is made available to You free of charge, Avaya Enterprise Customers will pay Avaya for Your use of the Avaya Digital ID when You interact with such companies) and related purposes.

The above Personal Data will form part of Your Avaya Digital ID. If You do not provide Avaya with Your Personal Data, You will not be able to use AMI. In particular, You will not be able to (i) create Your Avaya Digital ID to securely store, update and maintain Your Personal Data; (ii) use Your Avaya Digital ID as a tool to prove Your identity to respective companies.

2. For what general business purposes do We use Your Personal Data?

Your Personal Data collected through AMI will be used for the specific purpose(s) identified in Section 1 *"What types of Your Personal Data do We process?"* of this Privacy Statement or, otherwise, in the notice to You prior to Personal Data collection or as permitted by applicable law. Our general business purposes in processing Your Personal Data are as follows:

- To identify/authenticate You and operate AMI

  Your Avaya Digital ID and associated Personal Data will be used to identify and authenticate You when You interact with Avaya Enterprise Customers which have subscribed to AMI. Once You create Your Avaya Digital ID and start interacting with such companies, they will be notified (at a time You make a call) that You have Your Avaya Digital ID account activated that can serve as one of the means to verify Your identity.

- To maintain contact with You

  Avaya stores Your Personal Data so that We can communicate with You in the present (as We transact current business, e.g., to follow up on any of Your questions and requests for assistance or information), and in the future (as We uphold obligations and commitments resulting from the transacted business).

- To resolve disputes, enforce contracts and / or comply with our legal obligations

  This includes, but is not limited to, prevention and detection of fraud or misuse of AMI, maintain internal records, proofs of accepted legal terms or granted consents/permissions, authentication attempts, etc.

3. What is our legal basis for processing Your Personal Data?

Before processing Personal Data You provide Us, it is Our policy first to get Your consent to create Your Avaya Digital ID and allow You to use it for authentication purposes.

- You have a right to withdraw Your consent to use Avaya Digital ID at any time

  You will be able withdraw Your consent for the use of AMI by requesting Us to delete Your Avaya Digital ID at which point the Personal Data that could directly identify Yourself will be anonymized or deleted (for more information, please see Section 5 "*How long do We keep Your Personal Data?"* of this Privacy Statement). Access Your Avaya Digital ID (via AMI web application; Account Management tab) to initiate such request. Once such a request is processed, You will lose access to AMI and will not be able to rely on Your Avaya Digital ID for authentication purposes.

- Enrollment with Avaya Enterprise Customers

  You will have to enroll with each Avaya Enterprise Customer to be able to use Your Avaya Digital ID for authentication purposes with that legal entity. Once You create Your Avaya Digital ID and for the first time interact with a respective Avaya Enterprise Customer that has subscribed to the AMI service, You will be asked to choose to (i) proceed with the enrollment process, or (ii) enroll at a later date/time. If You enroll, then, depending on how Avaya Enterprise Customers have customized the AMI authentication preferences, Your subsequent calls to such Avaya Enterprise Customer may automatically involve a particular authentication challenge via AMI. You will be able to change Your enrollment preferences at any time by accessing Your Avaya Digital ID via the AMI web application (Account Management tab).

For any other processing operations, We may rely on other applicable legal basis (if required by applicable privacy laws), including our legitimate interest to fulfill the commercial and/or business purposes, such as: to detect security incidents, to protect against malicious, deceptive, fraudulent, or illegal activity; to debug to identify and repair errors that impair existing intended functionality; to undertake activities to verify or maintain the quality or safety of a service; to maintain, improve, upgrade, or enhance the service; to engage third-party sub-processors to perform the service, including maintaining and servicing Your Avaya Digital ID account, processing or fulfilling Your transactions, verifying Your information, etc.

4. What are Your rights to control Your Personal Data?

Depending on the applicable data protection laws, You may be granted the rights to control how Your Personal Data is used, stored, protected, etc. Access Your Avaya Digital ID (via AMI web application; Account Management tab) to implement Your rights or send Us an email to dataprivacy@avaya.com so We may assist You. If You exercise any of the rights granted by the respective privacy laws against Avaya – We will not discriminate against You in terms of providing equal AMI service in comparison to the other data subjects who have not exercised their rights. Here are the summaries (i.e., the list below is not exhaustive) of some of the rights We believe might be the most important to You while using AMI:

- The right to delete Avaya Digital ID

  You can request to delete Your Avaya Digital ID, at which point the Personal Data that could directly identify You will be anonymized or deleted (for more information see Section 5 "*How long do We keep Your Personal Data?"* of this Privacy Statement).

- The right to correct inaccurate Personal Data

  If You discover that Your Avaya Digital ID has details about You (i.e., Your name and/or email address) that are not factually correct, You can update them. For security reasons You will not be able to correct Your phone number or Your biometrics (i.e., face-print or voice-print) that You provided during the registration process. However, You will be allowed to add a new phone number and/or device which will require a re-keying process (for more information, please review the FAQ document available via the AMI web application).

- The right to know regarding the collection and use of Personal Data

You have a right to know (i) the categories of Personal Data We have collected about You; (ii) the categories of sources from which Your Personal Data is collected; (iii) the business or commercial purpose for collecting Your Personal Data; (iii) the categories of third parties with whom We share Your Personal Data - please review Section 1 *"What types of Your Personal Data do We process?"*, Section 2 *"How do We use Your Personal Data?"* and Section 8 *"Do We disclose Your Personal Data to 3rd parties?"* of this Privacy Statement to familiarize Yourself with this information.

- The right to access specific pieces of Personal Data

  In addition to Your "right to know," You may request to access the particular pieces of Personal Data We have collected about You.

- The right to data portability

  You have a right to receive the Personal Data You have provided Us with.

- The right to lodge a complaint

  If You have a complaint about privacy practices at Avaya, please contact Avaya Global Privacy Office (either by email at dataprivacy@avaya.com or by postal mail at Avaya Global Privacy Office, Avaya UK, Building 1000, Cathedral Square, Cathedral Hill, Guildford, Surrey GU2 7YL, United Kingdom). Its members will take reasonable endeavors to work with You to attempt to resolve Your complaint. You may also lodge a complaint with a respective supervisory authority and/or bring proceedings before a court of competent jurisdiction in accordance with the applicable data protection laws. Please review our Binding Corporate Rules Policies (available for a review at https://www.avaya.com/en/privacy/bcr/) for detailed information regarding the complaint-handling procedure at Avaya.

Other important information:

- Your other rights

  If, depending on the applicable data protection law, additional rights are granted to You, they are not exempted by this Privacy Statement.

- Limitations

  Please note that some of Your rights to access the Personal Data that We hold about You are not absolute. Personal Data may have been encrypted (and, therefore, may not be accessible to Us), erased or made anonymous in accordance with our obligations and practices, or there may be instances where applicable law or regulatory requirements allow or require Us to refuse to comply with Your request and/or disclose some or all of the Personal Data that We hold about You.

- Verification

  If You do not submit Your request to Us via AMI web application, We will need to obtain respective information (such as Your phone number, name, email address, etc.) along with a signed declaration, under penalty of perjury, that You are who You say You are, to locate You in our records and/or verify Your identity depending on the nature of the request.

- Your rights and Avaya Enterprise Customers

  Please note that Avaya will not be responsible, nor have control over what Avaya Enterprise Customer(s) will do with Your Personal Data once it is provided over to them - please refer to such companies for their privacy statements and policies. Your rights granted above are not extended by Avaya to the respective Avaya Enterprise Customers. You may contact them to enforce Your rights granted to You by applicable privacy laws.

5. How long do We keep Your Personal Data?

Avaya will retain and use Your Personal Data as required to accomplish the purposes for which it was collected or as necessary to resolve disputes, enforce contracts, and/or comply with our legal obligations.

If You (i) request to delete Your Avaya Digital ID, or (ii) do not use Your Avaya Digital ID account for interaction with Avaya Enterprise Customers (that have subscribed to the AMI) for 12 (twelve) consecutive months, Avaya will delete (or anonymize) Your Personal Data within Your Avaya Digital ID that could directly identify Yourself (e.g., Your name, email address, biometric voice, and facial samples). Notwithstanding the foregoing, Avaya may keep Your phone number, IDaaS Identity ID and other pseudonymized data stored on blockchain and associated with Your Avaya Digital ID for up to 6 (six) years to defend against legal claims (such Personal Data will not be used for any other purpose) or as required by applicable law (You may contact Avaya for additional information about the specific retention periods which may apply); following such term the foregoing Personal Data will be deleted (from our databases), automatically making the other pseudonymized Personal Data stored blockchain anonymous.

6. Is Your Personal Data safe?

Avaya relies on commercially reasonable security measures, including encryption, to protect Your Personal Data from identity theft or fraud. However, in the event of a security breach, Avaya will take relevant measures to remedy such breach without undue delay. Depending on the applicable jurisdiction, We may be obliged by law to inform You and/or relevant data protection authorities about breaches of security in our IT network, which may have affected Your Personal Data. Where legally required and possible, We will notify You (e.g., by sending an email or otherwise contacting You) and/or display a notice on our AMI web application in case of such a breach and You consent to receive such notices.

7. Is automated decision-making in scope?

- Logic involved

  AMI is fundamentally a mobile-centric service that heavily relies upon the use of a caller's device. AMI strongly leverages voice and facial recognition technologies for the purpose of authenticating mobile callers with a reasonable degree of confidence. This means that Your biometrics (i.e., face-print and voice-print) associated with Your Avaya Digital ID will be compared against the new biometrics You provide Us with during each and every subsequent authentication session; on top of this AMI will check whether the device You are using for authentication purposes holds the unique IDaaS Identity ID and private encryption key which were generated as a result of creation of Your Avaya Digital ID. If authentication results match (i.e., baseline threshold for use in determining whether a biometric check has been passed successfully), Your identity is likely to be verified resulting in successful authentication, otherwise, the authentication and identity verification may fail. The latter may be influenced, for example, by environment conditions (e.g., noisy environments can impact the effectiveness of voice biometrics; poorly lit areas can impact the effectiveness of facial recognition, etc.).

- Envisaged consequences

  If AMI is unable to authenticate You (for whatever reason), the respective Avaya Enterprise Customer may reject the transaction in question or request other means (if any) for proving Your identity. In case of any identification/authentication issues via AMI, please make sure that Your Avaya Digital ID holds Your most recent Personal Data (You have a right to update Your certain information – see Section 4 above titled *"What are Your rights to control Your Personal Data?"*) or contact the respective Avaya Enterprise Customer to seek additional authentication method(s). For more information, please review the FAQ document available via the AMI web application.

8. Do We disclose or sell Your Personal Data to 3rd parties?

In the preceding 12 months We have disclosed respective Personal Data categories (listed in Section 1 *"What types of Your Personal Data We process?"* of this Privacy Statement, subject to some exceptions enumerated below) for a business purpose(s) to the following parties:

- Avaya Enterprise Customers that have subscribed to AMI

  The primary purpose of AMI is to empower You to manage Your own digital identity and for You to authenticate Yourself to the respective Avaya Enterprise Customer that has subscribed to AMI and which will pay Avaya for Your use of the Avaya Digital ID when You interact with such company. We only transfer Your Personal Data to such third parties based on Your direct instructions and/or intentional actions. Avaya has executed respective contractual arrangements to cover the transfer of Personal Data to such third parties; however, Avaya is not be responsible for the privacy practices of such third-parties with whom You interact. For authentication and billing purposes Your Personal Data, such as name, phone number, unique IDaaS Identity ID, enrolment status, authentication attempts/results, are provided to the respective Avaya Enterprise Customer You interact with.

- Avaya (global) affiliates

  To ensure transfers of Personal Data required to deliver/support the AMI service are safeguarded legally, Avaya complies with its Binding Corporate Rules available for a review at https://www.avaya.com/en/privacy/bcr/.

- External third-party sub-processors (sub-contractors)

  Sub-processors (sub-contractors) access Your Personal Data to the extent necessary to perform their functions while supporting the AMI solution. Avaya does not transfer Your Personal Data to the third-party sub-processors (sub-contractors) unless they are bound to the respective security and data privacy requirements.

Specific disclosure rules to other third parties. Avaya may also disclose certain Personal Data to third parties in other particular instances, including (i) as required to do so by law, such as to comply with a court order or similar legal process; (ii) when We believe in good faith that disclosure is necessary to protect our rights, Your safety or the safety of others or defend against legal claims; (iii) for the purposes of prevention of fraud or other crime; (iv) in connection with or during negotiation of any merger, acquisition, sale of all or a portion of our assets, financing, liquidation, reorganization; and (v) in aggregated and/or anonymized form which can no longer be used to identify You.

Avaya does not sell and in the preceding 12 months has not sold Personal Data collected during the provisioning of the AMI service to third parties. Notwithstanding the foregoing, the following shall not be considered as a *"sale of data"* for the purpose of this Privacy Statement (i) disclosure (for identification purposes) of Your Personal Data to respective sub-contractors/sub-processors, including Avaya global affiliates, provided that such disclosure is reasonably necessary and proportionate to provide and support AMI; (ii) the disclosure of Your Personal Data to Avaya Enterprise Customers because Avaya only transfers Your Personal Data to a third party based on Your direct instructions and intentional actions when You interact with such company. For the purpose of this Section *"sell"* means any sharing or disclosure of Your Personal Data to a third party in exchange for monetary or other valuable consideration

9. Are international data transfers in scope?

Please note that Avaya operates globally and, therefore, the other parties (e.g., Avaya global affiliates and/or external third-party sub-contractors/sub-processors) might be established in countries which may have different privacy laws than in Your country of residence. However, Avaya follows relevant requirements (to the extent applicable) to make sure that such transfers are safeguarded legally.

10. Where do We store Your Personal Data?

The data centers are located within the US. However, Avaya holds the right to transfer the data to any other data centers located globally, provided Avaya complies with applicable privacy laws and regulations.

11. Privacy Statement update procedure

Avaya may modify this Privacy Statement at any time at its sole discretion to the extent required to comply with, among other things (a) laws or regulations applicable to AMI, (b) governmental orders, (c) modifications to AMI, (d) obligations imposed by Avaya suppliers, by posting the modified Privacy Statement on the AMI web application and / or upon

notice to You via email or through some other means designated by Avaya. Changes to this Privacy Statement will be effective as of the date Avaya posts them, unless Avaya specifies a different effective date when Avaya makes a particular change. You are solely responsible for checking for any updates for the Privacy Statement. Your continued use of AMI means that You accept and agree to any revised this Privacy Statement. In the event You do not agree to any such modification, Your sole and exclusive remedy is to discontinue using AMI and by requesting to delete Your Avaya Digital ID within fifteen (15) business days after Avaya posts the modified Privacy Statement.

12. Interpretation of this Privacy Statement

Any interpretation of this Privacy Statement will be done by the Avaya Global Privacy Officer. This Privacy Statement does not create or confer upon any individual any rights or impose upon Avaya any obligations outside of, or in addition to, any rights or obligations imposed by the privacy laws applicable to such individual's Personal Data. Should there be, in a specific case, any inconsistency between this Privacy Statement and such privacy laws, this Privacy Statement shall be interpreted to comply with such privacy laws.

13. Further information and contact details of the Avaya Global Privacy Office

If You have any questions or concerns about the privacy practices We have implemented within AMI, please contact the Avaya Global Privacy Office at dataprivacy@avaya.com or by postal mail to Avaya Global Privacy Office, Avaya UK, Building 1000, Cathedral Square, Cathedral Hill, Guildford, Surrey GU2 7YL, United Kingdom.

- END OF THE PRIVACY STATEMENT -