

## AVAYA BIOMETRIC DATA PROCESSING TERMS

The Avaya Biometric Data Processing Terms (herein after “Terms”) supplements any agreement (including but not limited to statements of works, service descriptions, attachments, schedules, and/or exhibits between Avaya and Customer for the purchase of services or other technology solutions from Avaya to the extent that Customer is located in a country that has applicable Biometric Laws and the Solution purchased that Customer is located in a country that has applicable Biometric Laws contains biometric capabilities that capture and process Biometric Data, of Biometric Users of the Biometric Service. The Biometric Service may use algorithms and other technologies to create Biometric Information, which may be considered biometric data under applicable biometric privacy laws.

THESE TERMS ARE SUBJECT TO CHANGE FROM TIME TO TIME IN AVAYA’S SOLE DISCRETION WITH SUCH CHANGES BEING EFFECTIVE UPON POSITING AT <https://support.avaya.com/LicenseInfo> (OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA). ANY USE OF THE BIOMETRIC SERVICE AFTER SUCH MODIFICATION SHALL CONSTITUTE ACCEPTANCE OF SUCH MODIFICATION.

### 1. DEFINITIONS

**1.1** For the purpose of these Terms the following shall also apply: (i) “**Avaya**” means Avaya LLC a Delaware corporation with an address of 350 Mt. Kemble Avenue Morristown, NJ 079604 or the appropriate Avaya affiliate or permitted assignee providing the Biometric Service to the Customer (“Avaya”). “**Biometric Data**” means any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. “**Biometric Information**” means any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual. Biometric Information does not include information derived from items or procedures excluded under the definition of biometric identifiers. “**Biometric Laws**” means all state, federal, and international biometrics laws including, but not limited to, 740 ILCS 14/10 et seq. (i.e., the Biometric Information Privacy Act (“BIPA”)), Rev. Code Wash. § 19.375.010 et seq., and Tex. Bus. & Com. Code § 503.001. “**Biometrics Service**” means a service provided by Avaya to Customer involving Biometric Data. “**Biometric User**” means individual end users about whom Biometric Data is created in connection with the Biometric Solution.

### 2. PROCESSING BIOMETRIC DATA ON BEHALF OF CUSTOMER

**2.1** Any collecting, capturing, receipt or otherwise obtaining of Biometric Data (“**Processing**”) by Avaya under these Terms shall occur only at the direction of the Customer (including when Processing is initiated by Customer’s users); and in accordance with these Terms, and for the purpose of fulfillment of Customer’s instructions.

### 3. COLLECTION OF BIOMETRIC DATA

**3.1** Customer is responsible for compliance with applicable law governing any collection, storage, use and/or transmission of Biometric Data that Customer conducts or facilitates while using Biometric Service. To the extent required by law, Customer will obtain written authorization from each Biometric User that Customer is providing such Biometric Data to Avaya, specifying the purpose and length of time for which Biometric User’s Biometric Data will be collected, stored, used, and/or transmitted and for what purpose, prior to the collection of such data.

**3.2** If requested by Avaya, Customer will: (i) provide to Avaya copies of the Biometric Users consents or releases collected and retained by Customer as required by this section and/or biometric privacy laws; and/or (ii) certify in writing to Avaya that such consents or releases have been obtained

### 4. STORAGE/RETENTION OF BIOMETRIC DATA

**4.1** Customer and Avaya agree that they shall use a reasonable standard of care consistent with Biometric Laws to store, transmit and protect from disclosure any Biometric Data. Such storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which the parties stores, transmits and protects from disclosure other confidential and sensitive information, including personal information that can be used to uniquely identify an individual or an individual’s account or property, such as genetic markers, genetic testing information, account numbers, PINs, driver’s license numbers and social security numbers.

**4.2** Customer will work with Avaya to ensure that Biometric Data is retained and purged in accordance with applicable law by: (a) deleting Biometric Data where self-service is available; or (b) providing timely notification to Avaya of the satisfaction of the purpose for which Biometric Data was collected with respect to any given Biometric User. Avaya is not responsible for Customer’s failure to provide timely notification of the termination of the satisfaction of the purpose for which Biometric Data was collected with respect to any given Biometric User.

**4.3** Customer’s Biometric Data (including any copy of it) shall be kept until the purpose for which the Biometric Data was collected is satisfied or one (1) year from receipt of Biometric Data from Customer, whichever period is shorter.

### 5. DISCLOSURE

**5.1** Avaya will not disclose, disseminate and/or transmit any Customer’s Biometric User’s Biometric Data to any person or entity other than the Customer without/unless:

**5.2** First having the Customer’s Biometrics User written consent.

**5.3** The disclosed information completes a financial transaction authorized by the Customer’s Biometric user;

**5.4** Disclosure is required by applicable state, federal, or international law; or

**5.5** Disclosure is required pursuant to a valid warrant or subpoena.

### 6. TERMINATION PROVISIONS FOR BIOMETRIC SERVICES.

**6.1** If Avaya determines that Customer has failed to comply with Biometric Laws or these Terms, Avaya may, in its sole discretion and upon notice to Customer, immediately suspend or terminate the Biometric Services.