

AVAYA VENDOR PRIVACY STANDARDS

Processing of Personal Data

1. **Standard:** Supplier shall process Personal Data only in accordance with Avaya's written instructions pursuant to Supplier's agreement with Avaya, this Section and any model contracts executed pursuant to Section 5, below.
2. **Ownership and Control:** Avaya retains all right, title, and interest in and to any Personal Data.
 - i) Supplier shall process all Personal Data on behalf of, and solely under the direction and control of, and pursuant to the instructions of, Avaya.
 - ii) Avaya grants Supplier for the term of this Agreement a limited, revocable and non-exclusive license to use Personal Data for those purposes necessary for Supplier to perform its obligations under this Agreement and for no other purpose.
3. **Supplier Requirements:** Supplier agrees that at any and all times during which it is Processing Personal Data from Avaya, or otherwise having access to such Personal Data, it will, without prejudice to Section 2:
 - (i) Take all appropriate and commercially reasonable Technical and Organizational Security Measures including physical, electronic, and procedural safeguards to protect the Personal Data against unauthorized or unlawful Processing of Personal Data and against a Data Security Breach so that the measures taken ensure a level of security appropriate to the harm that might result from such processing and the nature of the data to be protected;
 - (ii) Comply with all applicable privacy and data protection laws to which it is subject;
 - (iii) Not sell, share, or otherwise transfer or disclose any Personal Data received from Avaya to any other party without prior written consent from Avaya;
 - (iv) Not sub-contract the processing of Personal Data without the prior written consent of Avaya;
 - (v) As requested by Avaya, take all reasonable steps to (at Avaya's option) return, destroy, or arrange for the destruction of, Personal Data received from Avaya at the termination or expiration of this Agreement or when

informed by Avaya that there is no longer any legitimate business need to retain such Personal Data and supply Avaya with a written certificate signed by Supplier's Chief Compliance Officer confirming that the provisions of this Section 3(v) have been complied with;

- (vi) Ensure that Personal Data is available only to its employees who have a legitimate business need to access the Personal Data, who are bound by legally enforceable confidentiality obligations, and who have received training in data protection law and the appropriate Processing of Personal Data; and
- (vii) Assist and cooperate with Avaya fully and promptly with any necessary or appropriate disclosures, requests, notices or with other remedial measures as a result of any Data Security Breach.

4. **Supplier Reporting Obligations:** Supplier shall, within two business days, inform Avaya, in writing, as provided in the Notices section of this Agreement:

- (i) if it cannot comply with any provision of this Agreement, including this Section. If this occurs, Avaya shall be entitled to suspend the Processing of Personal Data, to terminate any of Supplier's further Processing of Personal Data and to terminate the Agreement in its entirety, with Supplier to cover Avaya's cost of obtaining comparable replacement services for those terminated services covered by this Agreement;
- (ii) of any request for access to any Personal Data from any government official, including any data protection agency or law enforcement agency;
- (iii) of any Data Security Breach involving Personal Data, including all relevant facts with respect to the Data Security Breach;
- (iv) in advance of any disclosure of Personal Data to a third party; and
- (v) of any and all requests, complaints or other communications received from any individual pertaining to their Personal Data and/or the processing of it. Supplier understands that it is not authorized to respond to these requests, unless explicitly authorized by Avaya, except for the request received from a governmental agency with a subpoena or similar legal document compelling disclosure by Supplier.

5. **European Union Compliance:** If requested by Avaya, Supplier agrees that it will execute a version of a model contract deemed by the European Commission, on the basis of Article 26 (4) of Directive 95/46/EC, to offer sufficient data protection safeguards as required by Article 26(2) of the Directive, unless Supplier has certified its adherence to the Safe Harbor negotiated by the United States Department of Commerce and the European Union or the Personal Data processing is in accordance with a European Commission decision that the third country in which the processing will take place provides adequate protection.

During the term of this Agreement, at Avaya's request, Supplier agrees that it will promptly execute any additional model contract documentation deemed by the European Commission to be necessary to provide sufficient data protection safeguards.

6. **Indemnification:** Notwithstanding any other provision in this Agreement to the contrary, Supplier shall indemnify, defend and hold harmless Avaya from and against any and all liabilities, costs, damages, expenses, attorneys' fees, computer forensic examinations, and/or amounts payable under any judgment, verdict, court order, or settlement for any breach of these Privacy Standards including without limitation any Data Security Breach involving Personal Data.
7. **Risk Assessment:** Upon Avaya's request, Supplier will provide evidence that it has established and maintains Technical and Organizational Security Measures governing the Processing of Personal Data appropriate to the risks represented by the Processing and the nature of the data to be protected. Avaya shall have the right to obtain from Supplier, and Supplier agrees to provide Avaya with, copies of and/or information concerning Supplier's information security protocols, and Avaya shall have the right to conduct reasonable inspections and/or audits of Supplier's information security protocols, and Supplier agrees to cooperate with Avaya regarding such inspections or audits.
8. **Definitions:** The following definitions shall apply to this standard:
 - (i) "Data Security Breach" means the unintentional loss of Personal Data, the inadvertent disclosure of Personal Data, and/or the unauthorized access to or unlawful or unauthorized processing or transfer of Personal Data or any other type of information security breach, loss or corruption involving Personal Data.
 - (ii) "Personal Data" means any information supplied by Avaya, or collected or generated by the Supplier on behalf of Avaya, that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, human resources identification number, physical characteristics or description, home or business address or location, email address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, supervisor name or medical or health information. For the avoidance of doubt, any data falling within the definition of "personal data" for the purpose of European Directive 95/46/EC, and its national implementations (as applicable) comes within the definition of Personal Data.
 - (iii) "Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration,

retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

- (iv) “Technical and Organizational Security Measures” means measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.