Last updated: 20 May 2021

Global Binding Corporate Rules:

Processor Policy

Contents

INTRODUCTION

This Global Binding Corporate Rules: Processor Policy ("**Processor Policy**") establishes Avaya's approach to compliance with data protection law when processing[1] personal information[2] on behalf of and under the instructions of a Controller and specifically with regard to transfers of personal information between members of the Avaya group of entities. This Processor Policy describes how Avaya will comply with data protection law in respect of processing it performs as a processor.

In this Processor Policy, we use the term "**Avaya**" to refer to Avaya group members ("**Group Members**") (a list of which is available at Appendix 1).

This Processor Policy does not replace any specific data protection requirements that might apply to a business unit or function.

This Processor Policy is accessible on Avaya's corporate website at www.avaya.com

[1] "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[2] "Personal information" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

PART I: BACKGROUND AND SCOPE

WHAT IS DATA PROTECTION LAW?

Data protection law gives individuals certain rights in connection with the way in which their personal information is processed. If organizations do not comply with data protection law, they may be subject to sanctions and penalties imposed by the national data protection authorities and the courts. When Avaya processes personal information to provide a service to a Controller, this activity and the personal information in question are covered and regulated by data protection law.

When an organization processes personal information for its own purposes, that organization is deemed to be a "*controller*" of that information and is therefore primarily responsible for meeting the legal requirements under data protection law.

On the other hand, when an organization processes personal information on behalf of a controller (for example, content hosted on behalf of an Avaya enterprise customer) that organization is deemed to be a "*processor*" of the information. In this case, the controller of the personal information (i.e. Avaya's customer) will be primarily responsible for meeting the legal requirements.

HOW DOES DATA PROTECTION LAW AFFECT AVAYA INTERNATIONALLY?

Data protection laws in the European Economic Area (EEA)[3] prohibit the transfer of personal information to countries outside the EEAthat do not ensure an adequate level of data protection. Some of the countries in which Avaya operates are not regarded by data protection authorities in the EEA as providing an adequate level of protection for individuals' privacy and data protection rights.

WHAT IS AVAYA DOING ABOUT IT?

Avaya must take proper steps to ensure that it processes personal information on an international basis in a safe and lawful manner. This Processor Policy therefore sets out a framework to satisfy data protection law requirements and in particular, to provide an adequate level of protection for all personal information processed by Avaya globally, either where the personal information is collected by a controller in the EEA, or where the personal information is collected by a Group Member in the EEA as a processor.

SCOPE OF THIS PROCESSOR POLICY

The standards described in this Processor Policy are worldwide standards that apply to all Group Members when processing any personal information as a processor. As such, Sections A and B of this Processor Policy apply regardless of the origin of the personal information that is processed by Avaya. Section C applies only to individuals whose personal information is processed by a Controller in the EEA and then transferred to a Group Member outside the EEA.

This Processor Policy applies to all personal information that Avaya is processing on behalf of a Controller which is not a Group Member, such as for instance in the context of providing a service to a business customer (e.g. personal information contained within content uploaded onto Avaya's cloud management

[3] For the purpose of this Processor Policy, reference to the term EEA means the member states of the European Union, plus Norway, Iceland and Lichtenstein.

platform by Avaya's business customers) (referred to as the "**Controller**" in this Processor Policy). More details about the material scope of this Processor Policy are provided in Appendix 10.

Avaya will apply this Processor Policy in all cases where Avaya processes personal information both manually and by automatic means.

AVAYA'S RESPONSIBILITY TOWARDS A CONTROLLER

When Avaya acts as a processor, the Controller on whose behalf Avaya is processing personal information is responsible for complying with data protection law. Certain data protection obligations are passed on to Avaya in the contracts or other legally binding document Avaya has with a Controller. Consequently, if Avaya fails to comply with the terms of the contract or other legally binding document it enters into with the Controller, the Controller may be in breach of applicable data protection law and Avaya may face a claim for breach of contract, which may result in the payment of compensation or other judicial remedies.

In such cases, if a Controller demonstrates that it has suffered damage, and that it is likely that the damage has occurred due to a breach of this Processor Policy by a Group Member outside the EEA (or a third party sub-processor established outside the EEA), the Avaya entity accepting liability (namely Avaya Deutschland GmbH) will be responsible for demonstrating that the Avaya entity outside the EEA (or the third party sub-processor established outside the EEA) is not responsible for the breach, or that no such breach took place.

Controllers must decide whether the commitments made by Avaya in this Processor Policy provide adequate safeguards for the personal information transferred to Avaya under the terms of the contract or other legally binding document they enter into with Avaya. Avaya will apply the Rules contained in this Processor Policy whenever it acts as a processor on behalf of a Controller. Where a Controller relies upon this Processor Policy as providing adequate safeguards, a copy of this Processor Policy will be incorporated into the contract or other legally binding document Avaya enters into with the Controller. If a Controller chooses not to rely upon this Processor Policy that Controller is responsible for putting in place another adequate safeguard to protect the personal information.

LEGALLY BINDING EFFECT OF THIS PROCESSOR POLICY

All Group Members and their employees (including new hires, individual contractors and temporary staff) worldwide must comply with, and respect, this Processor Policy when processing personal information as a processor, irrespective of the country in which they are located.

All Group Members who process personal information as a processor must comply with the Rules set out in **Part II** of this Processor Policy together with the policies and procedures set out in the appendices in **Part III** of this Processor Policy.

FURTHER INFORMATION

If you have any questions regarding the provisions of this Processor Policy, your rights under this Processor Policy or any other data protection issues you can contact Avaya's Data Privacy Office at the address below who will either deal with the matter or forward it to the appropriate person or department within Avaya.

Attention:	Data Privacy Officer
Email:	dataprivacy@avaya.com
Address:	Building 1000, Cathedral Square, Cathedral Hill, Guildford, Surrey GU2 7YL, United Kingdom

Avaya's Data Privacy Core Team is responsible for ensuring that changes to this Processor Policy are notified to the Controllers and to individuals whose personal information is processed by Avaya in accordance with Appendix 8.

If you are unhappy about the way in which Avaya has used your personal information, Avaya has a separate complaint handling procedure which is set out in Appendix 6.

PART II: PROCESSOR OBLIGATIONS

This Processor Policy applies in all situations where a Group Member processes personal information as a processor.

Part II of this Processor Policy is divided into four sections:

- Section A addresses the basic principles that Avaya must observe when it processes personal information as a processor.
- Section B deals with certain practical data protection commitments made by Avaya in connection with this Processor Policy.
- Section C describes the third party beneficiary rights that Avaya grants to individuals in its capacity as a processor under this Processor Policy.
- Section D explains Avaya's responsibility for breaches of this Controller Policy by Group Members outside of the EEA.

SECTION A: BASIC PRINCIPLES

RULE 1 – LAWFULNESS OF THE PROCESSING

Rule 1A – Avaya will ensure that all processing is carried out in accordance with applicable laws.

Avaya will comply with any applicable legislation, including any laws governing the protection of personal information. Where there is no data protection law, or where the law does not meet the standards set out by the Processor Policy, Avaya will process personal information in accordance with the Rules in this Processor Policy.

To the extent that any applicable data protection legislation requires a higher level of protection than is provided for in this Processor Policy, Avaya acknowledges that it will take precedence over this Processor Policy.

Avaya will ensure all processing of personal data has a legal basis (such as the individual's consent, the necessity to execute the terms of a contract, or the obligation to comply with an applicable law) in compliance with any applicable legislation, including any laws governing the protection of personal information in the country where the data is originally collected, and with the terms of the contract or other legally binding document Avaya has in place with the Controller.

Rule 1B – Avaya will cooperate and assist a Controller to comply with its obligations under applicable data protection laws without undue delay and to the extent reasonably possible.

Avaya will, without undue delay and as required under the terms of the contract or other legally binding document it has with a Controller, assist that Controller to comply with its obligations under applicable data protection laws, whether Avaya is processing the personal information as a processor or a sub-processor. This may include, for example, a responsibility to comply with certain instructions stipulated in the contract

or other legally binding document with a Controller, such as providing assistance to that Controller to meet its obligations to keep personal information accurate and up to date.

RULE 2 – FAIRNESS AND TRANSPARENCY

Rule 2 – Avaya will assist a Controller to comply with the requirement to inform and explain to individuals how their personal information will be processed in accordance with applicable laws.

The Controller has a duty to inform and explain to individuals, at the time their personal information is collected, or shortly after, how their information will be processed. This is usually done by means of an easily accessible fair processing statement. Avaya will provide such assistance and information to a Controller as may be required under the terms of the contract or other legally binding document it has with that Controller to comply with this requirement. For example, Avaya may be required to provide information about any sub-processors appointed by Avaya to process personal information on behalf of the Controller under the terms of the contract or other legally binding document with a particular Controller.

RULE 3 – PURPOSE LIMITATION

Rule 3 – Avaya will only process personal information on behalf of, and in accordance with, the instructions of the Controller.

Avaya will only process personal information on behalf of the Controller and in compliance with the terms of the contract or other legally binding document with that Controller unless Avaya is otherwise required to do so by Union or Member State law to which it is subject. In such a case, Avaya shall inform the Customer of that legal requirement before processing takes place, unless that law prohibits such information on important grounds of public interest. If in our opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions, Avaya shall immediately inform the Customer.

If, for any reason, Avaya is unable to comply with this Rule or its obligations under this Processor Policy in respect of any contract or other legally binding document it may have with a Controller, Avaya will inform the Controller promptly of this fact. The Controller may then suspend the transfer of personal information to Avaya and/or terminate the contract or other legally binding document, in accordance with the terms of the contract or other legally binding document it has with Avaya.

In such circumstances, or more generally upon termination of the provision of services related to the processing, Avaya will act in accordance with the instructions of the Controller and return, destroy or store the personal information, including any copies of the personal information, in a secure manner or as otherwise required, in accordance with the terms of the contract or other legally binding document it has with that Controller.

In the event that legislation prevents Avaya from returning the personal information to a Controller, or destroying it, Avaya will maintain the confidentiality of the personal information and will not process the personal information otherwise than in accordance with the terms of the contract or other legally binding document it has with that Controller.

RULE 4 – DATA MINIMIZATION AND ACCURACY

Rule 4 – Avaya will assist a Controller to keep the personal information accurate and up to date.

Avaya will comply with any instructions from a Controller, as required under the terms of the contract or other legally binding document with that Controller, in order to assist that Controller to comply with its obligation to keep personal information accurate and up to date.

RULE 5 – LIMITED RETENTION OF PERSONAL INFORMATION

Rule 5 – Avaya will only keep personal information for as long as is necessary under the terms of the contract or other legally binding document with a Controller.

When required to do so on instruction from a Controller, as required under the terms of the contract or other legally binding document with that Controller, Avaya will delete, anonymise, update or correct personal information.

Avaya will notify other Group Members or any third party sub-processor to whom the personal information has been disclosed accordingly so that they can also update their records.

In practice, when Avaya acts for a business customer in its capacity as the provider of a cloud content management and file sharing platform, Avaya does not have access to the personal information of its business customer and so, when acting in this capacity, Avaya is unlikely to be required to delete, anonymise, update or correct such personal information.

RULE 6 – SECURITY AND CONFIDENTIALITY

Rule 6A – Avaya will implement appropriate technical and organizational measures to safeguard personal information processed on behalf of a Controller.

Avaya will implement appropriate technical and organizational measures to protect personal information against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where processing involves transmission of personal information over a network, and against all other unlawful forms of processing.

Avaya will do so in accordance with the contract or other legally binding document it has with the Controller and in accordance with the laws of the country applicable to the Controller.

Rule 6B – Avaya will notify a Controller without undue delay of any security breach affecting the personal information that is being processed on behalf of a Controller in accordance with the terms of the contract or other legally binding document with that Controller.

Avaya will notify a Controller of any security breach in relation to personal information processed on behalf of that Controller without undue delay and as required to do so under the terms of the contract or other legally binding document it has with that Controller. Where applicable, Avaya shall assist the Customer to comply with its data security breach notification obligations, taking into account the nature of processing and information available to us.

Rule 6C – Avaya will comply with the requirements of a Controller regarding the appointment of any sub-processor.

Avaya will inform a Controller where processing undertaken on its behalf will be conducted by an internal or external sub-processor and will comply with the particular requirements of a Controller with regard to the appointment of sub-processors as set out under the terms of the contract or other legally binding document with that Controller. Avaya will ensure that up to date information regarding its appointment of sub-processors (both internal and external) is available to those Controllers at all times so that their general consent is obtained. If, on reviewing this information, a Controller objects to the appointment of a sub-processor to process personal information on its behalf, that Controller will be entitled to take such steps as are consistent with the terms of the contract or other legally binding document with Avaya and as referred to in Rule 3 of this Processor Policy.

Rule 6D – Avaya will ensure that sub-processors undertake to comply with provisions that are consistent with (i) the terms of the contract or other legally binding document it has with a Controller and (ii) this Processor Policy, and in particular that the sub-processor will adopt appropriate and equivalent security measures.

Avaya will only appoint sub-processors who provide sufficient guarantees in respect of the commitments made by Avaya in this Processor Policy. In particular, such sub-processors must be able to provide appropriate technical and organizational measures that will govern their use of the personal information to which they will have access in accordance with the terms of the contract or other legally binding document Avaya has with the Controller.

To comply with this Rule, where a sub-processor has access to personal information processed on behalf of Avaya, Avaya will take steps to ensure that it has in place appropriate technical and organizational security measures to safeguard the personal information and will impose strict contractual obligations, in writing, on the sub-processor, which provide:

- commitments on the part of the sub-processor regarding the security of that information, consistent with those contained in this Processor Policy and with the terms of the contract or other legally binding document Avaya has with the Controller in respect of the processing in question;
- that the sub-processor will act only on Avaya's instructions when processing that information; and
- such obligations as may be necessary to ensure that the commitments on the part of the sub-processor reflect those made by Avaya in this Processor Policy, and which, in particular, provide for adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals in respect of transfers of personal information from a Group Member in the EEA to a sub-processor established outside the EEA (including any onward transfers of personal information).

RULE 7 – RIGHTS OF INDIVIDUALS

Rule 7 – Avaya will assist Controllers to comply with their duty to respect the rights of individuals.

Avaya will act in accordance with the instructions of a Controller as required under the terms of the contract or other legally binding document with that Controller and undertake any necessary measures to enable a Controller to comply with its duty to respect the rights of individuals. In particular, if Avaya receives a request from an individual to exercise his/her rights, Avaya will transfer such request promptly to the Controller and not respond to such a request unless authorised to do so or required by law. Avaya will follow the steps set out in the Data Subject Rights Procedure (see Appendix 2) when dealing with such requests.

RULE 8 – ACCOUNTABILITY

Rule 8A – Avaya shall demonstrate compliance to the Controller.

Avaya shall make available to the Controller all information necessary to demonstrate compliance with its obligations under applicable data protection laws.

Rule 8B – Avaya will maintain records of data processing activities it is carrying out on behalf of a Controller.

Avaya shall maintain and update a record of all the processing activities carried out on behalf of a Controller and shall make such record available to the data protection authorities on request.

Rule 8C – Avaya shall assist the Controller in implementing privacy by design and privacy by default tools.

Avaya shall assist the Controller in implementing appropriate technical and organisational measures to comply with data protection principles, in particular to implement privacy by design and privacy by default tools and mechanisms.

SECTION B: PRACTICAL COMMITMENTS

RULE 9 – STAFF AND SUPPORT

Rule 9 – Avaya has appropriate staff and support to ensure and oversee privacy compliance throughout the business.

Avaya has appointed its Data Privacy Officer to oversee and ensure compliance with this Processor Policy supported by Privacy Stewards at regional, country and business unit level who are responsible for overseeing and enabling compliance with this Processor Policy on a day-to-day basis. A summary of the roles and responsibilities of Avaya's Data Privacy Core Team is set out in Appendix 3.

Avaya's Data Protection Officer receives the support of the highest management within Avaya. The group DPO reports directly to Avaya's General Counsel who is a member of the Executive Team and is accountable to Avaya's Board of Directors on all material or strategic issues relating to Avaya's compliance with Applicable Data Protection Laws and the Controller Policy. The group DPO also reports issues directly to Avaya's independent audit committee.

RULE 10 – PRIVACY TRAINING

Rule 10 – Avaya provides appropriate privacy training to employees who have permanent or regular access to personal information, who are involved in the processing of personal information or in the development of tools used to process personal information in accordance with the Privacy Training Program set out in Appendix 4.

Avaya provides appropriate privacy training to employees who:

- have permanent or regular access to Personal Information; or
- are involved in the Processing of Personal Information or in the development of tools used to Process Personal Information.

Avaya provides such training in accordance with the Privacy Training Program set out in Appendix 4.

RULE 11 – AUDIT

Rule 11 – Avaya will verify compliance with this Processor Policy and will carry out data protection audits on a regular basis in accordance with the Audit Protocol set out in Appendix 5.

Avaya will carry out data protection audits on a regular basis, which may be conducted by either internal or external accredited auditors. In addition, Avaya may conduct data protection audits on specific request from the Data Protection Officer. Such audits will cover all aspects of this Processor Policy (including methods of ensuring that corrective actions will take place).

Our customers may also audit Avaya (or any sub-processors acting on our behalf) to ensure we comply with our obligations under this Processor Policy in respect of the processing we carry out on behalf of customer, in accordance with the terms of customer's contract with us.

Avaya will conduct any such audits in accordance with the Audit Protocol set out in Appendix 5. This includes providing a copy of the data protection reports to the Group DPO and to Avaya's Board of Directors' Audit Committee and to the competent data protection authorities upon request. The competent data protection authorities may audit Group Members for compliance with the Processor Policy (including any related procedures and controls) in accordance with the Cooperation Procedure (see Appendix 7).

RULE 12 – COMPLAINT HANDLING

Rule 12 – Avaya will ensure that individuals may exercise their right to lodge a complaint and will handle such complaints in accordance with the Complaint Handling Procedure set out in Appendix 6.

Avaya will enable individuals to raise data protection complaints and concerns (including complaints about processing under this Processor Policy) with Avaya's Data Privacy Core Team, with the competent Data Protection Authorities or with the competent national courts, by complying with the Complaint Handling Procedure set out in Appendix 6. In particular, individuals may contact Avaya's Data Privacy Core Team at dataprivacy@avaya.com who will respond without undue delay and in any event within one month, unless

an extension of two additional months is needed by Avaya, taking into account the complexity and number of the requests.

RULE 13 – COOPERATION WITH DATA PROTECTION AUTHORITIES

Rule 13 – Avaya will cooperate with the data protection authorities on any issue related to the Processor Policy in accordance with the Cooperation Procedure set out in Appendix 7.

Avaya will cooperate with the competent data protection authorities for the Controller by complying with the Cooperation Procedure set out in Appendix 7 and will abide by a formal decision of any competent data protection authority[4] on any issues relating to the interpretation and application of the Processor Policy. Group Members may appeal any formal decision of any competent data protection authority in accordance with the laws of the country in which the competent data protection authority is established.

RULE 14 – UPDATE OF THE PROCESSOR POLICY

Rule 14 – Avaya will report changes to this Processor Policy to the data protection authorities in accordance with the Updating Procedure set out in Appendix 8.

Avaya will update this Processor Policy in accordance with the Updating Procedure set out in Appendix 8.

RULE 15 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE PROCESSOR POLICY

Rule 15A – Avaya will ensure that where it believes that the legislation applicable to it may prevent it from fulfilling its obligations under this Processor Policy or under the contract with the Customer, or such legislation has a substantial effect on its ability to comply with the Processor Policy, Avaya will promptly inform (unless otherwise prohibited by law):

- **Controller as provided for by Rule 3 (unless otherwise prohibited by a law enforcement authority);**
- **Data Privacy Officer and the EU entity with data protection responsibilities; and**
- **appropriate data protection authority competent for the Controller and for Avaya.**

Rule 15B – Avaya will ensure that where it receives a legally binding request for disclosure of personal information by a law enforcement authority or state security body which is subject to this Processor Policy, Avaya will:

- **notify the Controller promptly unless prohibited from doing so by a law enforcement authority; and**
- **put the request on hold and notify the lead data protection authority and the appropriate data protection authority competent for the Controller unless prohibited from doing so by a law enforcement authority or state security body.**

[4] The term "data protection authority" refers to the competent supervisory authority in an EEA Member State

Avaya will use its best efforts to inform the requesting law enforcement authority or state security body about its obligations under the data protection laws of the EEA and to obtain the right to waive this prohibition. Where such prohibition cannot be waived, despite Avaya's efforts, Avaya will provide the competent data protection authorities with an annual report providing general information about any requests for disclosure it may have received from a requesting law enforcement authority or state security body, to the extent that Avaya has been authorized by said authority or body to disclose such information (in accordance with Appendix 9).

In no event shall transfers of personal information from any Group Member to any law enforcement, state security or other government authority be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

Under the data protection laws of the EEA, individuals whose personal information is processed in the EEA by a Group Member acting as a processor (an "**EEA Entity**") and/or transferred to a Group Member located outside the EEA under the Processor Policy (a "**Non-EEA Entity**") have certain rights. The principles that individuals may enforce as third party beneficiaries are those that are set out under Part I, section A of Part II, and Rules 12, 13 and 15 under section B of Part II of this Processor Policy. These individuals may enforce the Policy as third party beneficiaries where they cannot bring a claim against a Controller in respect of a breach of any of the commitments in this Policy by a Group Member (or by a sub-processor) acting as a processor because:

a) the Controller has factually disappeared or ceased to exist in law or has become insolvent; and

b) no successor entity has assumed the entire legal obligations of the Controller by contract or by operation of law.

In such cases, the individual's rights are as follows:

- *Complaints*: Individuals may complain to an EEA Entity in accordance with the Complaint Handling Procedure (set out in Appendix 6) and may lodge a complaint with an EEA data protection authority in the jurisdiction of their habitual residence, or place of work, or place of alleged infringement;

- *Proceedings:* Individuals have the right to an effective judicial remedy if their rights under this Processor policy have been infringed as a result of the processing of their personal information in non-compliance with this Processor Policy. Individuals may bring proceedings to enforce compliance with this Processor Policy before the competent courts of the EEA Member State (either the jurisdiction where the Controller or Processor is established) or where the individual has his/her habitual residence and in case of non-compliance with this Processor Policy by a non-EEA Entity against Avaya Deutschland GmbH before the courts of Germany;

- *Compensation:* Individuals who have suffered material or non-material damage as a result of an infringement of this Processor Policy have the right to receive compensation form the Processor for the damage suffered. In particular, in case of non-compliance with this Processor Policy by a non-EEA Entity or any third party processor which is established outside the EEA, individuals may exercise these rights and remedies against Avaya Deutschland GmbH and where appropriate, receive compensation from Avaya Deutschland GmbH for any material or non-material damage suffered as a result of a breach of this Processor Policy.

Avaya Deutschland GmbH agrees to remedy any damage caused and pay compensation due by a Non-EEA Entity in violation of this Processor Policy to such individuals in accordance with the determination of the court or other competent authority.

- *Transparency:* Individuals may obtain a copy of the Intra-group Agreement entered into by the Group Members upon request. This Processor Policy is publicly available at www.avaya.com.

Where a Non-EEA Entity acts as a processor on behalf of a third party Controller, then if an individual suffers damage and where that individual can demonstrate that it is likely that the damage has occurred because of a breach of this Processor Policy, the burden of proof to show that (i) a Non-EEA Entity; or (ii) any third party sub-processor who is established outside the EEA who is acting on behalf of a Non-EEA Entity is not responsible for the breach, or that no such breach took place, will rest with Avaya Deutschland GmbH.

Avaya Deutschland GmbH will ensure that any action necessary is taken to remedy any breach of this Processor Policy by a Non-EEA Entity or any third party processor which is established outside the EEA and which is processing personal information on behalf of a Controller.

SECTION D: RESPONSIBILITY FOR BREACHES BY NON-EEA GROUP MEMBERS

Avaya Deutschland GmbH will be responsible for ensuring that any action necessary is taken to remedy any breach of this Processor Policy by a non-EEA Group Member in accordance with the Complaint Handling Procedure (Appendix 7).

In particular:

- If an individual can demonstrate damage he or she has suffered because of a breach of this Processor Policy by a non-EEA Group Member, Avaya Deutschland GmbH shall have the burden of proof to show that the non-EEA Group Member is not responsible for the breach, or that no such breach took place;

- where a non-EEA Group Member fails to comply with this Processor Policy, the courts and other competent authorities of the EEA will have jurisdiction and individuals may exercise their rights and remedies above against Avaya Deutschland GmbH as if the breach of this Processor Policy had been caused by Avaya Deutschland GmbH. In this context, individuals may, where appropriate, receive compensation (as determined by a competent court or other competent authority) from Avaya Deutschland GmbH for any material or non-material damage suffered as a result of a breach of this Processor Policy.

Where Avaya is engaged by a customer to process personal information on its behalf and both are responsible for harm caused by the processing in breach of this Processor Policy, Avaya accepts that both Avaya and the Customer may be held liable for the entire damage in order to ensure effective compensation of the individual.

PART III: APPENDICES

APPENDIX 1: LIST OF AVAYA GROUP MEMBERS

APPENDIX 2: DATA SUBJECT RIGHTS PROCEDURE

APPENDIX 3: PRIVACY COMPLIANCE STRUCTURE

APPENDIX 4: PRIVACY TRAINING PROGRAM

APPENDIX 5: AUDIT PROTOCOL

APPENDIX 6: COMPLAINT HANDLING PROCEDURE

APPENDIX 7: COOPERATION PROCEDURE

APPENDIX 8: UPDATING PROCEDURE

APPENDIX 9: GOVERNMENT DATA REQUEST PROCEDURE

APPENDIX 10: MATERIAL SCOPE OF THE PROCESSOR POLICY

APPENDIX 1: List of Avaya Group Members

Name of entity	Registered address
Avaya (China) Communication Co. Ltd.	Suite 7-11, Level 3, Tower W1, The Towers, Oriental Plaza, No. 1 Bejing, 100738, China
Avaya (Dalian) Intelligent Communications Co., Ltd.	No. 23 Dalian Software Park East Road, Building 15, 8th Floor-Unit 1, Dalian, 116023, China
Avaya (Malaysia) Sdn. Bhd.	A-30-6 Level 30 and A-31-6 Level 31, Block A Menara UOA Bangsar, Kuala Lumpur, 59000, Malaysia
Avaya (Shanghai) Enterprise Management Co. Ltd.	109B, Building 2, No. 774 Changde Road, Jing An District, China
Avaya Argentina S. R. L.	Lavalle 1877, 1st Floor, Ciudad de Buenos Aires, Argentina
Avaya Australia Pty Ltd.	Level 1, 123 Epping Road, North Ryde, Sydney, NSW 2113, Australia
Avaya Austria GmbH	Donau City Strasse 11, 9th Floor, Vienna, 1220, Austria
Avaya Belgium SPRL	Atlantis Corner Building, Keizer Karellaan, 576, Avenue Charles Quint, Brussels, 1082, Belgium
Avaya Brasil LTDA.	Avenida Das Nacoes Unidas N 14.171-Ebony Tower, Sao Paula, 04794-000, Brazil
Avaya Canada Corp.	11 Allstate Parkway, Suite 200, Markham, Ontario, L3R 9T8, Canada
Avaya Chile Limitada	Regus Business Center, Alcantara 200, Piso 6, Los Condes, Santiago de Chile, Chile
Avaya CIS LLC	52 Kosmodamianskaya Nab, Bldg 3 Moscow, 115054, Russian Federation
Avaya Cloud Inc.	350 Mount Kemble Avenue, Morristown, New Jersey, 07960, United States of America
Avaya Cloud Limited	Unit 25-29, Mervue Business Park, Mervue, Galway, H91 A0H2, Ireland
Avaya Communication de Colombia S. A.	Cra.7, No 99-53, Piso 14, Bogota, Colombia
Avaya Communication de Mexico, S. A. de C. V.	Avenida Presidente Masaryk, No. 111 Sexto Piso, Colonia Chapultepec Morales, Delegacion Miguel Hidalgo, 11570, Mexico
Avaya Communication Israel Ltd.	Azrieli Business Center Holon, 26 Harokmim Street, Building - D, Holon, 5885849, Israel

Name of entity	Registered address
Avaya Comunicacion Espana S. L. U.	Paseo de la Castellana 216, Madrid, 28046, Spain
Avaya Czech Republic s. r. o.	Sokolovska 192,186 00, Prague 8, Czech Republic
Avaya d. o. o.	Branimirova 29/3, Zagreb, 10000, Croatia
Avaya Denmark ApS	Orestads Boulevard 73, 2300 Kobenhavn S. Denmark, 2300, Denmark
Avaya Deutschland GmbH	Theodor-Heuss-Allee 112, Frankfurt, 60486, Germany
Avaya Egypt LLC	REGUS, 47, Office Building, 4th Floor, Section 1, Street 90 - North, New Cairo, 5th Settlement, Cairo, 11835, Egypt
Avaya EMEA Ltd. (Greece Branch)	166A Kifissias Avenue & Sofokleous Street, Maroussi, Athens, Greece
Avaya EMEA Ltd. (Portugal Branch)	Alameda António Sérgio 22 - 11º, 1495-132 Miraflores, Algés, Portugal
Avaya EMEA Ltd. (Saudi Arabia Branch)	Tatweer Towers, Level 9, Tower 3, King Fahad Rd, PO Box 57543, Riyadh, 11584, Saudi Arabia
Avaya EMEA Ltd. (South Africa Branch)	16 Culcross Road, PO Box 70392, Bryanston 2021, South Africa
Avaya Enterprises S. R. L.	Calea Floreasca, Nr. 169A, Floreasca Plaza, Birou NR. Bucuresti Sectorul 1, 2076, Romania
Avaya Finland Oy	Teknobulevardi 3-5, Vantaa, 01530, Finland
Avaya France SAS	Immeuble Central Park,9 Rue Maurice Mallett, 92 130, Issy les Moulineaux Cedex, 92445, France
Avaya GmbH & Co. KG	Theodor-Heuss-Allee 112, Frankfurt, 60486, Germany
Avaya Holdings Corp.	4655 Great America Parkway, Santa Clara, California 95054 USA
Avaya Hong Kong Company Limited	Suite 2309, 23/F Cityplaza One, 1111 King's road, Hong Kong
Avaya Hungary Ltd. / Avaya Hungary Communication Limited Liability Company	West End City Center, B Tower, Vaci ut 1-3, Budapest 1062, Hungary
Avaya LLC	350 Mt. Kemble Avenue, Morristown, NJ 07960, United States of America
Avaya India Private Limited	202, Platina, 2nd Floor, Plot no. C-59, G-Block, Near Citi Bank, Bandra Kurla Complex, Mumbia, 400 051, India

Name of entity	Registered address
Avaya India Private Limited (Bangladesh Branch Office)	Faruque Rupayan Tower (18th Floor), Kemal Ataturk Avenue, Banani C/A, Dhaka, 1213, Bangladesh
Avaya India Private Limited (Sri Lanka Branch)	Level 26&34, East Tower, World Trade Centre, Echelon Square, Colombo, 00100, Sri Lanka
Avaya International Sales Limited	Unit 25-29 Mervue Business Park, Mervue, Galway, H91 A0H2, Ireland
Avaya Italia S. p. A.	Viale Edison 110/B, 20099 Sesto San Giovanni, Milan, Italy
Avaya Japan Ltd.	Akasaka Tameike Tower, 2-17-7, Akasaka, Minato-ku, Tokyo, 107-0052, Japan
Avaya Korea Ltd.	12/F Gangnum Finance Centre, 737 Yoksam-dong, Kangnam-gu, Seoul, 135-984, Korea
Avaya Luxembourg S. A. R. L.	99 Rue de Bonnevoie, 1260, Luxembourg
Avaya Nederland B. V.	Marconibaan 59, Nieuwegein, 3439 MR, Netherlands
Avaya Nederland B. V. (U. A. E. Branch)	Emirates Towers, Level 24, Sheikh Zayed Road, PO Box 72055, Dubai, United Arab Emirates
Avaya New Zealand Limited	Part Level 9, Telco Building, 16 Kingston Street, Auckland 1010, New Zealand
Avaya Nigeria Limited	St. Nicholas House, 10th Floor, Catholic Mission Street, Lagos, Nigeria
Avaya Norway AS	H Hayerdahld Gate 1, 0160, Oslo, Norway
Avaya Peru S. R. L.	Avenida Victor Andres Belaunde 147, Via Principal 140, Edificio Real 6, Piso 7, Centro Empresarial San Isidro, Lima 27, Peru
Avaya Philippines Inc.	14/F Tower 1, Enterprise Center, 6766 Ayala Avenue, Makati City, 1226, Philippines
Avaya Poland Sp. z. o. o.	Ul. Ilzecka 26, Warsaw, 02-135, Poland
Avaya Singapore Pte Ltd	89 Science Park Drive, #01-03/04, the Rutherford, Block A, Singapore Science Park, 118261, Singapore
Avaya Sweden AB	Farogatten 33 8tr, Kista, 16451, Sweden
Avaya Switzerland GmbH	Hertistrasse 31, Wallisellen, 8304, Switzerland
Avaya UK	Building 1000, Cathedral Square, Cathedral Hill, Guildford, Surrey GU2 7YL, United Kingdom
Avaya World Services Inc.	1209 Orange Street, Wilmington, Delaware, 19801, United States of America

Name of entity	Registered address
CAAS Technologies LLC	c/o Avaya, 350 Mt Kemble Avenue, PO BOX 1934, Morristown, New Jersey, 07960, United States of America
Esna Technologies Ltd.	c/o Smith & Williamson, 25, Moorgate, London, EC2R 6AY, United Kingdom
Esna Technologies Inc.	30 West Beaver Creek Road, Suite 101, Richmond Hill, Ontario, L4B 3K1, Canada
HyperQuality Inc.	c/o Avaya, 350 Mt Kemble Avenue, PO Box 1934, Morristown, New Jersey, 07960, United States of America
HyperQuality II LLC	2101, 4th Avenue, Suite 620, Seattle, Washington, 98121, United States of America
HyperQuality India Private Limited	34, Udyog Vihar, Gurgaon, Haryana, 120016, India
Intellisist Inc.	2101 4th Avenue, Suite 620, Seattle, Washington, 98121-2328, United States of America
KnoahSoft Technologies Private Limited	Level 12, Ph 5, Blk Vega, the V Ascendas IT Park Plot 17, Software Units Layout, Madhapur, Hyderabad, TG 500081, India
Konftel AB	Dobelngatan 19, Umea, 903 06, Sweden
PT Sierra Communication Indonesia	WISMA 46, 46th Floor, Unit No. 46.02, Jl. Jend. Sudirman Kav 1, Jakarta, 10220, Indonesia
Sierra Asia Pacific Inc. (Taiwan Branch)	12/F, Unit A, Union Enterprise Building, 109 Min Sheng East Road, Sec. 3, Taipei, Taiwan, 8520310, Province of China
Sierra Asia Pacific Inc. (Thailand Branch)	10th Floor Unit 10.05 - 06, Wave Place Building, 55 Wireless Road, Bangkok, 10330, Thailand

Appendix 2: Data Subject Rights Procedure

1. Introduction

1.1 Avaya's Processor Policy safeguards personal information transferred between Avaya's Group Members.

1.2 Individuals whose personal information is processed by Avaya under the Processor Policy have certain data protection rights, which they may exercise by making a request to the Controller of their personal information (a "**Request**").

1.3 This Data Subject Rights Procedure ("**Procedure**") explains how Avaya assists any customer ("**Controller**") to deal with a Request it receives from individuals whose Personal Information are Processed by Avaya as a Processor under the Processor Policy.

1.4 Where a Request is subject to data protection law in the EEA because it is made in respect of personal information processed in the EEA, such a Request will be dealt with by Avaya in accordance with this Procedure, unless the applicable data protection law differs from this Procedure, in which case the applicable data protection law will prevail.

2. Data subjects' data protection rights

2.1 An individual making a Request to the Controller is entitled to the following rights:

(a) **Right to information**: this is the right to be informed about the processing of personal information by the Controller, including the right to be informed about the existence of automated decision-making (including profiling) and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual;

(b) **Right of access**: this is the right to obtain confirmation as to whether the Controller is processing personal information about an individual and, if so, to be given a description of the personal information and to obtain a copy of the personal information being processed ;

(c) **Right to rectification**: This is the right for individuals to obtain rectification without undue delay of inaccurate Personal Information a Controller may process about them;

(d) **Right to erasure, rectification and to object**: This is the right to erasure of personal information, to restrict or to object to the processing on certain legal grounds, as well as their right to lodge a complaint with a data protection authority; and

(e) **Right to data portability**: this is the right for individuals to receive personal information about them from the Controller in a structured, commonly used and machine-readable format and to transmit that information to another Controller, if certain grounds apply.

3. Responsibility to assist the Controller to respond to a Request

3.1 The Controller of an individual's personal information is primarily responsible for responding to a Request and for helping the individual concerned to exercise his or her rights under applicable data protection laws.

3.2 As such, when an individual contacts Avaya to make any Request and where Avaya processes that individual's personal information as a Processor on behalf of a Controller under this Processor Policy, Avaya must inform the relevant Controller promptly and provide it with reasonable assistance to help the individual to exercise his or her rights in accordance with the Controller's duties under applicable data protection laws.

4. Initial assessment of a Request

4.1 Upon receiving any Request from an individual, Avaya will ensure all such Requests are immediately routed to the Data Privacy Core Team at dataprivacy@avaya.com. The Data Privacy Core Team will document the date on which such Request was received together with any other information that may assist the Data Privacy Core Team to deal with the Request.

4.2 The Data Privacy Core Team will assess whether Avaya is a Controller or Processor of the personal information that is the subject of the Request and:

(a) where the Data Privacy Core Team determines that Avaya is a Controller of the personal information, it will respond to the Request in accordance with the Binding Corporate Rules: Controller Policy ; and

(b) where the Data Privacy Core Team determines that Avaya is a Processor of the personal information on behalf of a Controller, it shall pass the Request promptly to the relevant Controller in accordance with its contract terms with that Controller and will not respond to the Request directly unless authorised to do so by the Controller.

4.3 When Avaya processes information on behalf of a Controller (for example, to provide a service or content hosted on behalf of an Avaya enterprise customer), Avaya is considered to be a processor of the information and the Controller will be primarily responsible for meeting the legal requirements. This means that when Avaya acts as a processor, the Controller retains the responsibility to comply with applicable data protection law.

4.4 Certain data protection obligations are passed to Avaya in the contract or other legally binding document Avaya has with a Controller. Avaya must act in accordance with the instructions of the Controller and undertake any reasonably necessary measures to enable the Controller to comply with its duty to respect the rights of individuals.

4.5 When Avaya rectifies, erases or ports personal information on instruction of a Controller when it is acting as a processor, Avaya will notify other Group Members or any sub-processor to whom the personal information has been disclosed accordingly so that they can also update their records, unless this proves impossible or involves disproportionate effort.

5. Questions about this Procedure

5.1 All queries relating to this Procedure are to be addressed to Avaya's Data Privacy Core Team at dataprivacy@avaya.com.

Appendix 3: Privacy Compliance Structure

1. Introduction

Avaya's compliance with global data protection laws and the Processor Policy is overseen and managed throughout all levels of the business by a global, multi-layered, cross-functional privacy compliance structure. Further information about Avaya's Privacy Compliance Structure is set out below and in the structure chart provided at Annex 1.

2. Data Privacy Officer

Avaya has appointed a Data Privacy Officer ("**DPO**") who provides executive-level oversight of, and has responsibility for, monitoring Avaya's compliance with applicable data protection laws and the Processor Policy. The DPO reports all material and strategic issues relating to Avaya's compliance with data protection laws and policies to the General Counsel, the deputy General Counsel and the Senior Director of Corporate Security, Ethics & Compliance in regular institutionalised meetings. The General Counsel is a member of the Executive Team and provides reports and is accountable to Avaya's independent Board of Directors and the Audit Committee of the Board of Directors. The General Counsel can raise privacy matters with the Board of Directors. Furthermore, the DPO also has access and reports issues directly to the Audit Committee of the Board of Directors. The DPO leads, and is supported by, Avaya's Data Privacy Core Team.

The DPO's key responsibilities include:

- Ensuring that the Processor Policy and other privacy related policies, objectives and standards are defined and communicated.
- Providing clear and visible senior management support and resources for the Processor Policy and for privacy objectives and initiatives in general.
- Evaluating, approving and prioritizing remedial actions consistent with the requirements of the Processor Policy, strategic plans, business objectives and regulatory requirements.
- Periodically assessing privacy initiatives, accomplishments, and resources to ensure continued effectiveness and improvement.
- Ensuring that Avaya's business objectives align with the Processor Policy and related privacy and information protection strategies, policies and practices.
- Facilitating communications on the Processor Policy and privacy topics with Avaya's Executive Team.
- Dealing with any escalated privacy complaints in accordance with the Appendix 6: Complaint Handling Procedure

3. Data Privacy Core Team

Avaya's Data Privacy Core Team comprises Avaya's DPO, , a senior compliance manager and other representatives from Avaya's Legal , and IT Teams. Incorporating members from Avaya's Legal and IT Teams ensures appropriate independence and oversight of duties relating to all aspects of Avaya's data protection compliance. The Data Privacy Core Team is accountable for managing and, together with the Business Data Privacy Stewards, implementing Avaya's data

privacy program internally (including the Processor Policy) and for ensuring that effective data privacy controls are in place for any third party service provider Avaya engages. In this way, the Data Privacy Core Team is actively engaged in addressing matters relating Avaya's privacy compliance on a routine, day-to-day basis. Its responsibilities include:

- Providing guidance to the Business Data Privacy Stewards about the processing of personal information subject to the Processor Policy and to assess, in conjunction with the Business Data Privacy Stewards, the processing of personal information by Avaya's Group Members for potential privacy-related risks.

- Responding to inquiries and compliance relating to the Processor Policy from employees, customers and other third parties raised through its dedicated e-mail address at dataprivacy@avaya.com.

- Working closely with Avaya's Privacy Stewards in driving the Processor Policy and related policies and practices at a functional and local country level, providing guidance and responding to privacy questions and issues.

- Providing input on audits of the Processor Policy, coordinating responses to audit findings and responding to inquiries of the data protection authorities.

- Monitoring changes to global privacy laws and ensuring that appropriate changes are made to the Processor Policy and Avaya's related policies and business practices.

- Overseeing training for employees on the Processor Policy and on data protection legal requirements in accordance with the requirements of Appendix 4: Privacy Training Program.

- Promoting the Processor Policy and privacy awareness across business units and functional areas through privacy communications and initiatives.

- Evaluating privacy processes and procedures to ensure that they are sustainable and effective.

- Reporting periodically on the status of the Processor Policy to the DPO.

- Ensuring that the commitments made by Avaya in relation to updating, and communicating updates to the Processor Policy as set out in Appendix 8: Updating Procedure are met.

- Overseeing compliance with Appendix 2: Data Subject Rights Procedure and the handling of requests made thereunder.

Avaya's Data Privacy Core team, and the team under the Senior Director of Corporate Security, Ethics and Compliance have a number of specific responsibilities in relation to the implementation and oversight of the Processor Policy and privacy matters more generally, including:

- Audit of attendance of privacy training courses as set out in Appendix 4: Privacy Training Program

- Ensuring that any issues or instances of non-compliance with the Processor Policy are brought to the attention of Avaya's Data Privacy Core Team and DPO and that any corrective actions are determined and implemented within a reasonable time.

Avaya's Internal Audit team is responsible for performing and/or overseeing independent audits of compliance with the Processor Policy as set out in Appendix 5: Audit Protocol, and ensuring that such audits address all aspects of the Processor Policy.

4. Privacy Committee

Avaya's Privacy Committee comprises Regional Data Privacy Stewards and Business Data Privacy Stewards. The Business Data Privacy Stewards will include functional leads or key representatives from the main functional areas within Avaya, including Compliance, Procurement & Vendor Management, Legal, Technical Operations, Engineering, Support, Marketing and Human Resources. The key responsibilities of the Privacy Committee include:

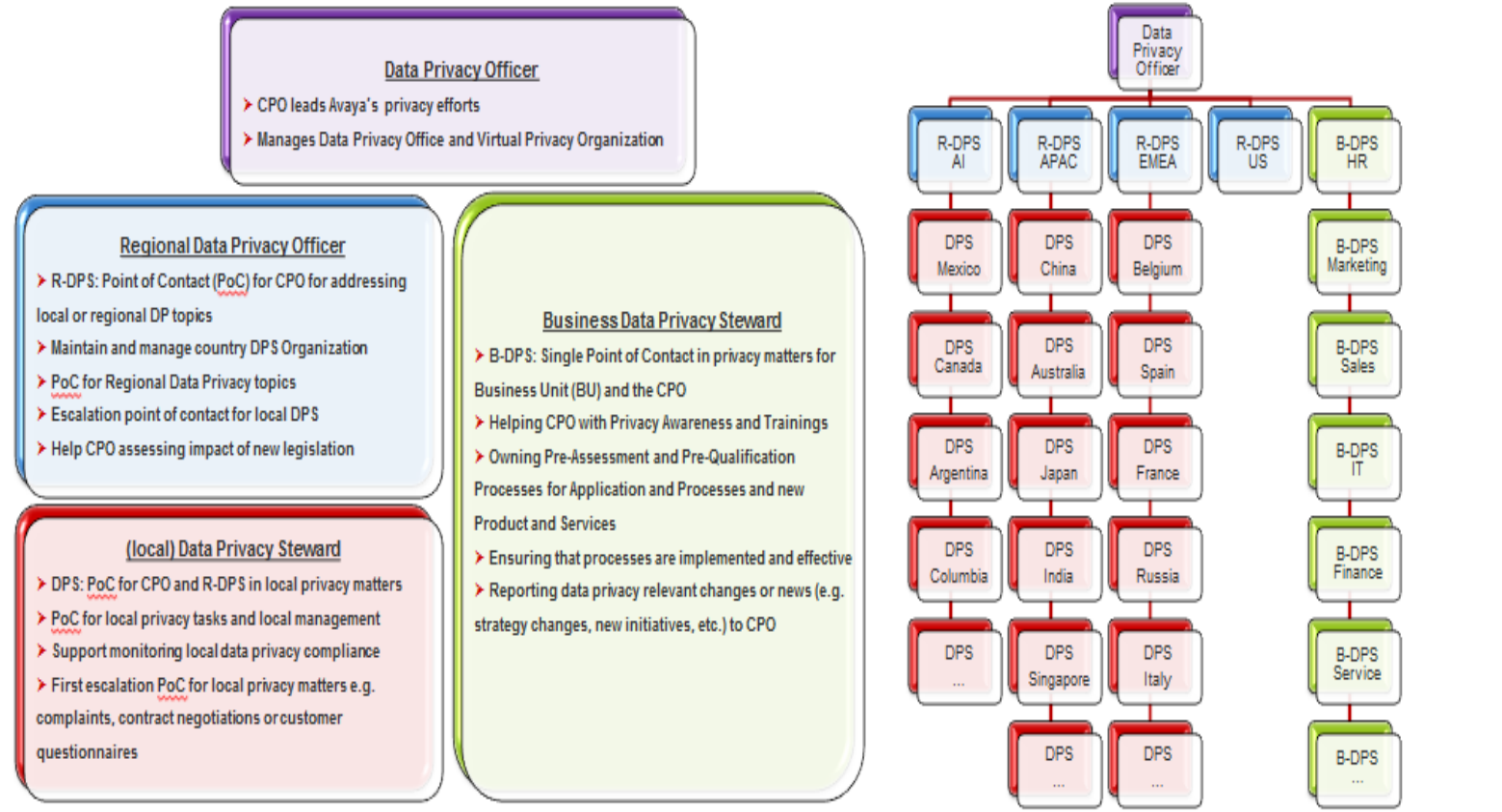
- Promoting the Processor Policy at all levels in their functional areas.
- Implementing Avaya's privacy policies (including the Processor Policy) within their respective areas of responsibility and assisting the Data Privacy Core Team with its enforcement.
- Escalating questions and compliance issues or communicating any actual or potential violation of the Processor Policy to the Data Privacy Core Team.
- Through its liaison with the Data Privacy Core Team, serving as a channel through which the Data Privacy Core Team can communicate data privacy compliance actions to all key functional areas of the business.

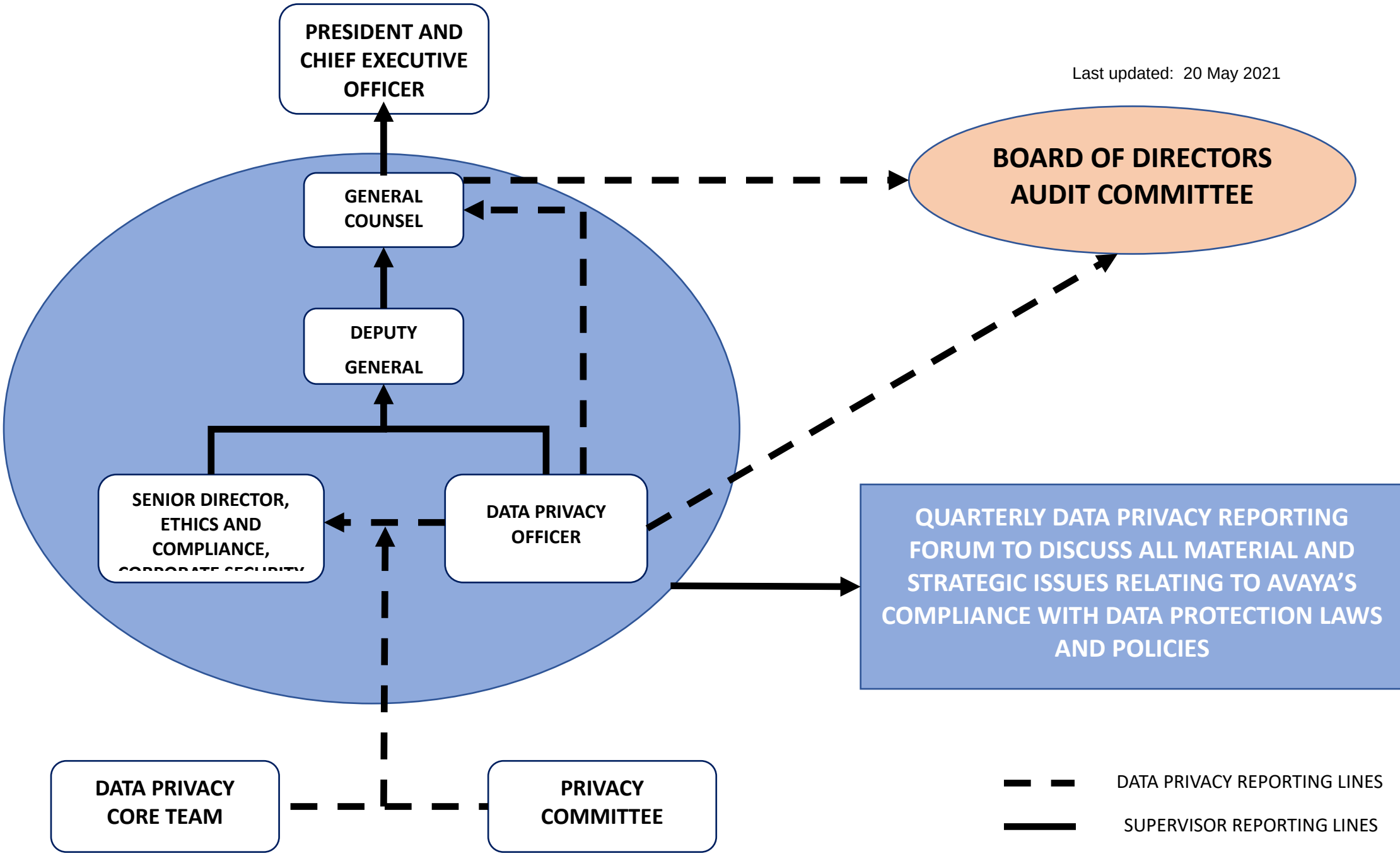
Avaya's Privacy Committee will meet on a formal and regular basis, at a minimum frequency of every six months, to ensure a coordinated approach to data protection compliance across all functions.

5. Avaya's Personnel

All personnel within Avaya are responsible for supporting the functional Privacy Committee on a day-to-day basis and adhering to Avaya's privacy policies (including the Processor Policy). In addition, Avaya personnel are responsible for escalating and communicating any potential violation of the privacy policies to the appropriate Privacy Steward or, if they prefer, Avaya's Data Privacy Core Team. On receipt of a notification of a potential violation of the privacy policy the issue will be investigated to determine if an actual violation occurred. Results of such investigations will be documented.

Annex 1: Overview of Avaya's Privacy Compliance Structure




PRESIDENT AND CHIEF EXECUTIVE OFFICER
Last updated: 20 May 2021
BOARD OF DIRECTORS AUDIT COMMITTEE
GENERAL COUNSEL
DEPUTY GENERAL
SENIOR DIRECTOR, ETHICS AND COMPLIANCE,
DATA PRIVACY OFFICER
QUARTERLY DATA PRIVACY REPORTING FORUM TO DISCUSS ALL MATERIAL AND STRATEGIC ISSUES RELATING TO AVAYA'S COMPLIANCE WITH DATA PROTECTION LAWS AND POLICIES
DATA PRIVACY CORE TEAM
PRIVACY COMMITTEE
DATA PRIVACY REPORTING LINES
SUPERVISOR REPORTING LINES

Appendix 4: Privacy Training Program

1. Background

1.1 This Appendix 4; Privacy Training Program provides a summary as to how Avaya trains its employees and contractors on the requirements of the Processor Policy.

1.2 Avaya trains employees (including new hires and contractors) whose roles will bring them into contact with personal information, on the basic principles of data protection, confidentiality and information security awareness. It also provides specific training on particular legal obligations, such as the Health Insurance Portability and Accountability Act of 1996 ('HIPAA') in the US, and requirements and best practices, such as those specified by the International Organization for Standards (ISO) 27001.

1.3 Employees who have permanent or regular access to personal information, who are involved in the collection of personal information or in the development of tools to process personal information receive additional, tailored training on the Processor Policy and specific data protection issues relevant to their role. This training is further described below and is repeated on a regular basis.

2. Responsibility for the Privacy Training Program

2.1 Avaya's Data Privacy Core Team and the team under the Senior Director of Corporate Security, Ethics and Compliance have overall responsibility for privacy training at Avaya, with input from other functional areas including Information Security, HR and other departments, as appropriate. They will review training from time to time to ensure it addresses all relevant aspects of the Processor Policy and that it is appropriate for individuals who have permanent or regular access to personal information, who are involved in the collection of personal information or in the development of tools to process personal information.

2.2 Avaya's senior management supports the attendance of the privacy training courses and is responsible for ensuring that individuals within the company are given appropriate time to attend and participate in such courses. Course attendance is monitored via regular audits of the training process. These audits are performed by Avaya's Data Privacy Core Team and the team under the Senior Director of Corporate Security, Ethics and Compliance and/or independent third party auditors.

2.3 In the event that these audits reveal persistent non-attendance, this will be escalated to Avaya's Data Privacy Officer for action. Such action may include escalation of non-attendance to the appropriate management authority within Avaya who will be responsible and held accountable for ensuring that the individual(s) concerned attend and actively participate in such training.

3. About the training courses

3.1 Avaya has developed mandatory electronic training courses, supplemented by face to face training for employees where appropriate. The courses are designed to be both informative and user-friendly, generating interest in the topics covered. Employees must correctly answer a series of multiple choice questions for the course to be deemed complete.

3.2 All Avaya employees will be required to complete the training:

(a) as part of their induction programme;

(b) as part of a regular refresher training at least once every two years (the timing of which is determined by the team under the Senior Director of Corporate Security, Ethics and Compliance); and

(c) when necessary based on changes in the law or to address any compliance issues arising from time to time.

3.3 Certain employees will receive specialist training, including those who are involved in particular processing activities such as employees who work in HR, Marketing, Product Development, Procurement and Customer Support or whose business activities include processing sensitive personal data. Specialist training is delivered as additional modules to the basic training package, which will be tailored depending on the course participants.

4. Training on the Processor Policy

4.1 Avaya's training on the Processor Policy will cover the following main areas:

4.1.1 Background and rationale:

(a) What is data protection law?

(b) How data protection law will affect Avaya internationally.

(c) The scope of the Processor Policy.

(d) Terminology and concepts.

4.1.2 The Processor Policy:

(a) An explanation of the Processor Policy.

(b) Practical examples.

(c) How to assist Controllers with respect to the individuals' rights under the Processor Policy.

(d) The privacy implications arising from processing personal information for clients.

4.1.3 Where relevant to an employee's role, training will cover the following procedures under the Processor Policy:

(a) Data Subject Rights Procedure, Appendix 2.

(b) Audit Protocol, Appendix 5.

(c) Complaint Handling Procedure, Appendix 6.

(d) Cooperation Procedure, Appendix 7.

(e) Updating Procedure, Appendix 8.

5. Further information

5.1 Any queries about training under the Processor Policy should be addressed to Avaya's Data Privacy Office at dataprivacy@avaya.com.

Appendix 5: Audit Protocol

1. Background

1.1 Avaya must audit its compliance with the Processor Policy on a regular basis, and the purpose of this Appendix 5: Audit Protocol is to describe how and when Avaya will perform such audits.

1.2 The role of Avaya's Data Privacy Core Team is to provide guidance about the collection and use of personal information subject to the Processor Policy and to assess the collection and use of personal information by Group Members for potential privacy-related risks. The collection and use of personal information with the potential for a significant privacy impact is, therefore, subject to detailed review and evaluation on an on-going basis. Accordingly, although this Audit Protocol describes the formal assessment process adopted by Avaya to ensure compliance with the Processor Policy as required by the data protection authorities, this is only one way in which Avaya ensures that the provisions of the Processor Policy are observed and corrective actions taken as required.

2. Approach

Overview of audit

2.1 Compliance with the Processor Policy is overseen on a day to day basis by Avaya's Data Privacy Core Team and the Business Data Privacy Stewards. In particular, Avaya's Data Privacy Core Team is responsible for providing input on audits of the Processor Policy and coordinating responses to audit findings as explained in Appendix 3.

Avaya's Internal Audit Team is responsible for performing and/or overseeing independent audits of compliance with the Processor Policy and will ensure that such audits address all aspects of the Processor Policy. . Avaya's Internal Audit Team is responsible for ensuring that any issues or instances of non-compliance are brought to the attention of the Data Privacy Core Team and Data Privacy Officer and that any corrective actions are determined and implemented within a reasonable time.

2.2 Where Avaya acts as a processor, Controllers (or auditors acting on their behalf) may audit Avaya for compliance with the commitments made in the Processor Policy and may extend such audits to any sub-processors acting on Avaya's behalf in respect of such processing, in accordance with the terms of the relevant contract or other legally binding document with Avaya.

Frequency of audit

2.3 Audits of compliance with the Processor Policy are conducted:

(1) at least annually in accordance with Avaya's audit procedures;

(2) at the request of the Data Privacy Officer and / or the Board of Directors;

(3) as determined necessary by Avaya's Data Privacy Core Team (for example, in response to a specific incident); or

(4) (with respect to audits of the Processor Policy), as required by the terms of the relevant contract or other legally binding document Avaya has entered with a Controller.

Scope of audit

2.4 Avaya's Internal Audit team will conduct a risk-based analysis to determine the scope of an audit, which will consider relevant criteria, such as: areas of current regulatory focus; areas of specific or new risk for the business; areas with changes to the systems or processes used to safeguard information; areas where there have been previous audit findings or complaints; the period since the last review; and the nature and location of the personal information processed.

2.5 In the event that a Controller exercises its right to audit Avaya for compliance with the Processor Policy, the scope of the audit shall be limited to the data processing facilities, data files and documentation relating to that Controller. Where Avaya is processing personal data on behalf of a customer who is the Controller, Avaya will not provide that Customer with access to systems which process personal information of other Controllers.

Auditors

2.6 Audit of the Processor Policy (including any related procedures and controls) will be undertaken by Avaya's Internal Audit team. In addition, Avaya may appoint independent and experienced professional auditors acting under a duty of confidence as necessary to perform audits of the Processor Policy (including any related procedures and controls) relating to data privacy.

2.7 In the event that a Controller exercises its right to audit Avaya for compliance with the Processor Policy, such audit may be undertaken by that Controller, or by independent and suitably experienced auditors selected by that Controller, as required by the terms of the relevant contract or other legally binding document with that Controller.

2.8 In addition Avaya agrees that EEA data protection authorities may audit Group Members for the purpose of reviewing compliance with the Processor Policy (including any related procedures and controls) in accordance with the terms of Appendix 7: Cooperation Procedure.

Reporting

2.9 Data privacy audit reports are submitted to the Data Privacy Officer and, to the Board of Directors. If the report reveals breaches or the potential for breaches of a serious nature (for example, presenting a risk of potential harm to individuals or to the business), a copy will be sent to the ultimate parent's Board of Directors

2.10 Upon request and subject to applicable law, Avaya will:

(a) provide copies of the results of data privacy audits of the Processor Policy (including any related procedures and controls) to a competent EEA data protection authority; and

(b) to the extent that an audit relates to personal information Avaya processes on behalf of a Controller, report the results of any audit of compliance with the Processor Policy to that Controller.

Avaya's Data Privacy Core Team is responsible for liaising with the EEA data protection authorities for the purpose of providing the information outlined in this section.

Appendix 6: Complaint Handling Procedure

1. Background

1.1 The purpose of this Appendix 6: Complaint Handling Procedure is to explain how complaints brought by an individual whose personal information is processed by Avaya under the Processor Policy are dealt with.

1.2 This procedure will be made available to individuals whose personal information is processed by Avaya on behalf of a Controller under the Processor Policy.

1.3 Where a complaint is brought in respect of the processing of personal information where Avaya is the processor in respect of that information, Avaya will communicate the details of the complaint to the Controller promptly and will act strictly in accordance with the terms of the contract or other legally binding document between the Controller and Avaya.

1.4 If the Controller requires that Avaya investigate the complaint, Avaya shall do so in accordance with section 3 of this Complaint Handling Procedure.

2. How individuals can bring complaints

2.1 Individuals can bring complaints in writing by contacting Avaya's Data Privacy Core Team either by email at dataprivacy@avaya.com or by postal mail at: Data Privacy Officer, Avaya House, Cathedral Hill, Guildford, Surrey, GU2 7YL, United Kingdom.

3. How complaints are handled by Avaya

Who handles complaints?

3.1 Avaya's Data Privacy Core Team will handle all complaints arising under the Processor Policy. Avaya's Data Privacy Core Team will liaise with colleagues from relevant business and support units as appropriate to deal the complaint.

What is the response time?

3.2 Avaya's Data Privacy Core Team will acknowledge receipt of a complaint to the individual concerned within five working days, investigating and making a substantive response within one month.

3.3 If, due to the complexity of the complaint, a substantive response cannot be given within this period, Avaya's Data Privacy Core Team will notify the complainant that Avaya cannot provide a prompt response and will provide a substantive response to the data subject within a maximum period of six months.

What happens if a complainant disputes a finding?

3.4 If the complainant disputes the response from Avaya's Data Privacy Core Team or any aspect of a finding and notifies Avaya's Data Privacy Core Team, the matter will be referred to Avaya's Data Privacy Officer ("**DPO**"). The DPO will review the case and advise the complainant of his or her decision either to accept the original finding or to substitute a new finding. The DPO will respond to the complainant within six months of the receipt of the complaint. As part of the review, the

DPO may arrange to meet the parties to the complaint in an attempt to resolve it. If, due to the complexity of the complaint, a substantive response cannot be given within this period, the DPO will advise the complainant accordingly and provide a reasonable estimate for the timescale within which a response will be provided which will not exceed three months from the date the complaint was referred.

3.5 If the complaint is upheld, the DPO will arrange for any necessary steps to be taken as a consequence.

4. Right to lodge a complaint to a data protection authority in the EEA and/or to bring proceedings before a court of competent jurisdiction

4.1 Individuals may lodge a complaint to a competent data protection authority of the individual's habitual residence, the data subject's place of work or the place of the alleged infringement.

4.2 Without prejudice to section 4.1, individuals have right to an effective judicial remedy and bring proceedings before a court of competent jurisdiction in accordance with the data protection laws applicable to them, whether or not they have first complained directly to Avaya.

4.3 If the matter relates to personal information which was collected and / or used by a Group Member in the EEA but then transferred to a Group Member outside the EEA and an individual wants to make a claim against Avaya, the claim may be made against the Group Member in the EEA responsible for exporting the personal information or the courts of the Member State where the individual has his or her habitual residence.

Appendix 7: Cooperation Procedure

1. Introduction

1.1 This Appendix 7: Cooperation Procedure sets out the way in which Avaya will cooperate with the data protection authority competent for the relevant Controller in relation to the Processor Policy.

2. Cooperation Procedure

2.1 Where required, Avaya will make the necessary personnel available for dialogue with a data protection authority competent for the relevant Controller in relation to the Processor Policy.

2.2 Avaya will actively review, consider and (as appropriate) implement:

(a) any decisions made by data protection authority competent for the relevant Controller on any data protection law issues that may affect the Processor Policy; and

(b) the views of the European Data Protection Board in connection with Binding Corporate Rules for Processors, as outlined in its published Binding Corporate Rules guidance.

2.3 Subject to applicable data protection laws, Avaya will provide copies of the results of the data protection audit of the Processor Policy (including any related procedures and controls) to a data protection authority competent for the relevant Controller.

2.4 Avaya agrees that:

(a) the data protection authorities may audit any Group Member for compliance with the Processor Policy, or request to receive access to the Group Member's data protection audit reports upon request, in accordance with the applicable data protection law(s) of their respective jurisdictions; and

(b) the data protection authority competent for the relevant Controller may audit any Group Member who processes personal information on behalf of a Controller established within the jurisdiction of that data protection authority for compliance with the Processor Policy, including obtaining access to that Group Member's premises and data processing equipment and means, subject to appropriate safeguards, including effective judicial remedy and due process and in accordance with the applicable procedural law(s) of that jurisdiction. Such audits should fully respect the confidentiality of the information obtained and the trade secrets of Avaya (unless this requirement is in conflict with local applicable law).

2.5 Avaya agrees to abide by a formal decision of the data protection authority competent for the relevant Controller on any issues relating to the interpretation and application of the Processor Policy. Avaya may appeal any formal decision of the competent data protection authority in accordance with the laws of the country in which the competent data protection authority is established.

Appendix 8: Updating Procedure

1. Introduction

1.1 This Appendix 8: Updating Procedure sets out the way in which Avaya will communicate changes to the Processor Policy to the competent data protection authorities, the Controllers and to the Group Members bound by the Processor Policy.

1.2 Any reference to Avaya in this procedure is to the Data Privacy Core Team which will ensure that the commitments made by Avaya in this procedure are met.

2. Material changes to the Processor Policy

2.1 Avaya will communicate any material changes to the Processor Policy (including any modification that would possibly affect the level of protection offered by the BCR or significantly affect the BCR including as a result of any change in applicable data protection laws) and to the list of Group Members bound by the Processor Policy without undue delay to the Lead Data Protection Authority and to any other relevant EEA data protection authorities as appropriate.

2.2 Where a change to the Processor Policy materially affects the conditions under which Avaya processes personal information on behalf of a Controller under the terms of its contract or the legally binding document it has with Avaya, Avaya will also communicate the proposed change to the affected Controller before it is implemented and with sufficient notice to enable the affected Controller to object. The Controller may then suspend the transfer of personal information to Avaya and/or terminate the contract or other legally binding document, in accordance with the terms of its contract or legally binding document with Avaya.

3. Administrative changes to the Processor Policy

3.1 Avaya will communicate changes to the Processor Policy which:

(a) are administrative in nature (including changes in the list of Group Members); or

(b) have occurred as a result of either a change of applicable data protection law in any EEA country or due to any legislative, court or supervisory authority measure,

to the Lead Data Protection Authority and to any other relevant data protection authorities in the EEA (as appropriate) at least once a year. Avaya will also provide a brief explanation to the Lead Data Protection Authority and to any other relevant data protection authorities of the reasons for any notified changes to the Processor Policy.

3.2 In addition, Avaya will make available changes to the Processor Policy which:

(a) are administrative in nature (including changes in the list of Group Members); or

(b) have occurred as a result of a change of applicable data protection law in any EEA country or due to any legislative, court or supervisory authority measure,

to any affected Controller on whose behalf Avaya processes personal information.

4. Communicating changes to the Processor Policy

4.1 Avaya will communicate all changes to the Processor Policy, whether administrative or material in nature and to the list of Group Members bound by the Processor Policy:

(a) to the Group Members bound by the Processor Policy via written notice (which may include e-mail); and

(b) systematically to Controllers who benefit from the Processor Policy via www.avaya.com.

4.2 Avaya's Data Privacy Officer will maintain an up to date list of Group Members bound by the Processor Policy and of the sub-processors appointed by Avaya to process personal information on behalf of Controllers. This information will be available on request from Avaya at dataprivacy@avaya.com.

5. Logging changes to the Processor Policy

5.1 The Processor Policy contains a change log which sets out the date at which the Policy is revised and the details of any revisions made. Avaya's Data Privacy Officer will maintain an up-to-date list of the changes made to the Processor Policy.

5.2 Avaya will also maintain an accurate and up-to-date list of all Group Members that are bound by the Processor Policy and are listed in Appendix 1. This information will be available on request from Avaya.

6. New Group Members

6.1 Avaya will ensure that all new Group Members are bound by and have implemented the Processor Policy before a transfer of personal information to them takes place.

Appendix 9: Government Data Request Procedure

1. Introduction

1.1 This Appendix 9: Government Data Request Procedure sets out Avaya's policy for responding to a request received from a law enforcement or other government authority (together the "**Requesting Authority**") to disclose personal information processed by Avaya on behalf of a Controller ("**Data Production Request**").

1.2 Where Avaya receives a Data Production Request, it will handle that Data Production Request in accordance with this procedure.

1.3 If applicable data protection law(s) require a higher standard of protection for personal information than is required by this procedure, Avaya will comply with the relevant requirements of applicable data protection law(s).

2. General principle on Data Production Requests

2.1 As a general principle, Avaya does not disclose personal information in response to a Data Production Request unless it is under a compelling legal obligation to make such disclosure.

2.2 Even where disclosure is required, Avaya's policy is that the Controller should have the opportunity to protect the personal information requested because it has the greatest interest in opposing, or is in the better position to comply with, a Data Production Request.

2.3 For that reason, unless it is legally compelled to do so, Avaya will report to the competent data protection authorities and provide the Controller with details of the Data Production Request. Avaya will cooperate with the competent data protection authorities and the Controller to address the Data Production Request.

3. Data Production Request review

3.1 Receipt of a Data Production Request

3.1.1 If Avaya receives a Data Production Request, the recipient of the request must pass it to Avaya's Data Privacy Officer immediately upon receipt, indicating the date on which it was received together with any other information which may assist Avaya's Data Privacy Officer to deal with the request.

3.1.2 The request does not have to be made in writing, made under a court order, or mention data protection law to qualify as a Data Production Request.

3.2 Initial steps

3.2.1 Avaya's Data Privacy Officer will carefully review each and every Data Production Request individually and on a case-by-case basis. Avaya's Data Privacy Officer will liaise with the legal department as appropriate to deal with the request to determine the nature, urgency, scope and validity of the Data Production Request under applicable laws and to identify whether action may be needed to challenge the Data Production Request.

4. Notice of a Data Production Request

4.1 Notice to the Controller

4.1.1 After assessing the nature, urgency, scope and validity of the Data Production Request, Avaya will notify and provide the Controller with the details of the Data Production Request prior to disclosing any personal information, unless legally prohibited.

4.2 Notice to the competent data protection authorities

4.2.1 Avaya will also put the request on hold in order to notify and report to the competent data protection authorities (including information about the data requested, the Requesting Authority, and the legal basis for the disclosure), unless legally prohibited.

4.2.2 Where Avaya is prohibited from notifying the competent data protection authorities and suspending the request, Avaya will use its best efforts (taking into account the nature, urgency, scope and validity of the request) to inform the Requesting Authority about its obligations under applicable data protection law(s) and to obtain the right to waive this prohibition. Such efforts may include asking the Requesting Authority to put the request on hold so that Avaya can consult with its competent data protection authorities and may also, in appropriate circumstances, include seeking a court order to this effect. Avaya will maintain a written record of the efforts it takes.

5. Transparency reports

5.1 In cases where Avaya is prohibited from notifying the competent data protection authorities about a Data Production Request, it commits to providing the competent data protection authorities with a confidential annual report (known as a Transparency Report), which reflects to the extent permitted by applicable laws, the number and type of Data Production Requests it has received for the preceding year and the Requesting Authorities who made those requests.

6. Bulk transfers

2.11 In no event will Avaya transfer Personal Information to a Requesting Authority in a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society.

6.1 **Queries**

6.2 All queries relating to this procedure are to be addressed to the Avaya's Data Privacy Office at dataprivacy@avaya.com.

Appendix 10: Material Scope of the Processor Policy

1. Background

1.1 Avaya's Processor Policy provides a framework for the transfer of Personal Information between Avaya's Group Members.

1.2 This document sets out the material scope of the Processor Policy. It specifies the data transfers or set of transfers, including the nature and categories of personal information, the type of processing and its purposes, the types of individuals affected, and the identification of the third country or countries.

2. Customer data

Who transfers the personal information described in this section?	Every Avaya Group Member inside of the European Economic Area ("**EEA**") may transfer the personal information that they process on behalf of a third-party Controller (referred to as the "Customer" within this Processor Policy) described in this section to every other Avaya Group Member inside and outside of the EEA. Every Group Member outside of the EEA may also transfer the personal information that they process on behalf of a Customer described in this section to every Avaya Group Member inside and outside of the EEA. Transfers made directly from a Customer (whether inside or outside of the EEA) directly to a Group Member as Processor (whether inside or outside of the EEA) will also be within the scope of the Processor Policy.
Who receives this personal information?	Every Avaya Group Member outside of the EEA may receive the personal information described in this section which is sent to them by other Avaya Group Members or Customers inside and outside of the EEA. Every Group Member inside of the EEA may also receive the personal information described in this section which is sent to them by other Avaya Group Members or Customers inside and outside of the EEA.

What categories of personal information are transferred?	The personal information transferred will comprise any personal information about an End User that a Customer chooses to share with Avaya for Processing, in particular within the context of the provision of services by Avaya to said Customer. Avaya does not determine or control the personal information about the End Users that Customers may choose to share with Avaya for processing. However, such personal information usually includes: - **Identification data** – name, user details. - **End-user account details** – address, telephone, email address, etc. - **Metadata –** time, date, duration, IP address, etc. - **Content data** – voice, text
What categories of sensitive personal information (if any) are transferred?	Avaya Group Members do not intentionally collect or process any sensitive personal information about End Users on behalf of Customers.
Who are the types of individuals whose personal information are transferred?	The types of individuals whose personal information are transferred will typically comprise any End Users whose personal information a Customer chooses to share with Avaya for Processing. Avaya does not determine or control the End Users about whom Customers may choose to share personal information with us.
Why is this personal information transferred and how will it be used?	Avaya will process this personal information as instructed by its Customers, in order to provide a service to its Customers. In particular, this personal information will be used to process or fulfil Customers' orders, including to: • give access to End Users to Avaya's services at the Customer's request; • support End Users on regarding their use of Avaya's services; • handle any claims or queries from End Users on behalf of a Customer.

Where is this personal information processed?	The personal information described in this section may be processed in every territory where Avaya Group Members or their internal or external processors are located. A list of Avaya Group Member locations is available at Appendix 1.